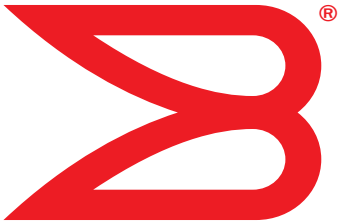
53-1002304-01
14 October 2011



Brocade FCX, Brocade FastIron SX, Brocade ICX 6610

Web Management Interface User Guide

Supporting Brocade FastIron v07.3.00

BROCADE

Copyright © 2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, BigIron, DCX, Fabric OS, FastIron, NetIron, SAN Health, ServerIron, and TurboIron are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Brocade Communications Systems, Incorporated

Corporate and Latin American Headquarters
Brocade Communications Systems, Inc.
130 Holger way
San Jose, CA 95134
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems China HK, Ltd.
No. 1 Guanghua Road
Chao Yang District
Units 2718 and 2818
Beijing 100020, China
Tel: +8610 6588 8888
Fax: +8610 6588 9999
E-mail: china-info@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour B - 4ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 5640
Fax: +41 22 799 5641
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems Co., Ltd. (Shenzhen WFOE)
Citic Plaza
No. 233 Tian He Road North
Unit 1308 – 13th Floor
Guangzhou, China
Tel: +8620 3891 2000
Fax: +8620 3891 2111
E-mail: china-info@brocade.com

Document History

Title	Publication number	Summary of changes	Date
FastIron CX and SX Web Management Interface User Guide	*53-1002191-01*	New document	February 2011
Brocade FCX, Brocade FastIron SX, Brocade ICX 6610 Web Management Interface User Guide	*53-1002304-01*	Updated for 07.3.00 release	October 2011

Contents

About This Document

In this chapter xiii
Audience xiii
Supported hardware and software xiii
Document conventions xiv
Text formatting xiv
Notes xiv
Notice to the reader xiv
Related publications xv
Getting technical help xv
Web access xv
E-mail and telephone access xv

Chapter 1 Getting Started with the Web GUI

In this chapter 1
Access requirements 1
Logging in to the Web Management Interface 2
Logging out of the Web Management Interface 4
Using the Web Management Interface 4
Web Management Interface areas 5

Section I Monitoring Device Performance and Metric

Chapter 2 Monitoring Basic Device Information

In this chapter 9
Displaying the ARP cache 9
Displaying the device information 10
Displaying flash information 13
Displaying memory information 13
Displaying the front panel 14
Status LED display 15
Displaying the front panel for Brocade FCX devices 15
Displaying the front panel for the Brocade ICX 6610 device . . 18
Displaying the front panel for Brocade FSX devices 18

Displaying MAC addresses 20
Displaying the system log 21

Chapter 3 Monitoring Stacks

In this chapter 25
Displaying the stack details 25
Displaying a stack module 27
Displaying stack neighbors. 28
Displaying stack ports information 29
Displaying stack port statistics 30
Displaying stack port interfaces. 31
Displaying stack resources. 32

Chapter 4 Monitoring Ports

In this chapter 35
Displaying Ethernet port statistics 35
Displaying Ethernet port attributes 37
Displaying Ethernet port utilization 39
Displaying the management port information 41
Displaying the management port real-time information 42
Displaying port inline power for Brocade FCX and Brocade ICX 6610 devices 44
Displaying inline power statistics 45
Displaying inline power details 47
Displaying port inline power for Brocade FSX devices 49

Chapter 5 Monitoring STP

In this chapter 51
Displaying STP information. 51

Chapter 6 Monitoring RSTP

In this chapter 55
Displaying RSTP information 55

Chapter 7 Monitoring IP

In this chapter 59
Displaying IP cache 59
Displaying IP traffic information for devices running Layer 2 code 60

Displaying IP traffic information for devices running Layer 3 code 64
Displaying the IP routing table 66

Chapter 8 Monitoring OSPF

In this chapter 69
Displaying the OSPF ABR ASBR router information 69
Displaying OSPF area information 71
Displaying OSPF external link-state database 73
Displaying the OSPF interfaces 75
Displaying OSPF link state database 78
Displaying OSPF neighbors 80
Displaying OSPF virtual interfaces 82
Displaying OSPF virtual neighbors 85

Chapter 9 Monitoring PIM

In this chapter 89
Displaying the PIM neighbors 89
Displaying the PIM virtual interface 90

Chapter 10 Monitoring DVMRP

In this chapter 93
Displaying DVMRP neighbors 93
Displaying DVMRP next hop entries 94
Displaying DVMRP routes 95
Displaying DVMRP virtual interfaces 96

Chapter 11 Monitoring BGP

In this chapter 99
Displaying BGP attributes 99
Displaying BGP neighbors 100
Displaying BGP route statistics 102
Displaying the BGP neighbor summary 104

Chapter 12 Monitoring Virtual Redundant Router

In this chapter 107
Displaying VRRP interfaces 107
Displaying VRRP virtual router entries 108

Displaying VRRP-E interfaces 110
Displaying VRRP-E virtual router entries 111
Displaying VSRP virtual switch entries 112

Chapter 13 Monitoring RMON

In this chapter 115
Displaying RMON history 115
Displaying RMON Ethernet statistics 117
Changing polling interval 120
Displaying RMON Ethernet error statistics 120

Section II Configuring Device Components

Chapter 14 Configuring Stack Components

In this chapter 125
Configuring the general settings for an IronStack 125
Modifying stack priority 126
Modifying stack ports 128
Configuring a stack module 129

Chapter 15 Configuring System Components

In this chapter 133
Configuring the system boot sequence for Brocade FCX and Brocade ICX 6610 devices 134
Configuring the system boot sequence for Brocade FSX devices . 135
Configuring the system clock 136
Configuring the general system settings 137
Configuring the system identification 139
Configuring the system IP address 140
Configuring a standard ACL 141
Configuring an extended ACL 142
Configuring an IP access group 144
Configuring the system MAC filter 145
Configuring a filter group 147
Configuring the maximum system parameter value 148
Configuring a system module 149
Configuring an NTP server 151
Configuring a RADIUS server 152

Configuring a TACACS/TACACS+ server 154
Configuring management authentication 155
Configuring management authorization 156
Configuring management accounting 157
Configuring an SNMP community string 158
Configuring the general management parameters 160
Configuring a management system log 161
Configuring a trap 164
Configuring a trap receiver 166
Configuring a management user account 168
Configuring the web management preference 169

Chapter 16 Configuring Module Components

In this chapter 171
Configuring a module 171
Modifying inline power budget 172

Chapter 17 Configuring Port Parameters

In this chapter 175
Configuring an Ethernet port 175
Configuring port inline power 177
Configuring a management port 178
Configuring the port uplink relative utilization 179

Chapter 18 Configuring Monitor and Mirror Port

In this chapter 181
Configuring a mirror port 181
Configuring a monitor port 182

Chapter 19 Configuring QoS

In this chapter 185
Configuring the QoS profile 185
Configuring the QoS profile bind 186

Chapter 20 Configuring VLAN

In this chapter 189
Configuring a port VLAN for Brocade FCX and Brocade ICX 6610 devices 189

Modifying a port VLAN 192
Configuring a port VLAN for Brocade FSX devices 194
Configuring a protocol VLAN 196
Configuring an IP subnet VLAN 199

Chapter 21 Configuring STP

In this chapter 201
Configuring STP parameters 201
Changing STP bridge parameters 201
Changing STP port parameters 204

Chapter 22 Configuring RSTP

In this chapter 207
Configuring RSTP parameters 207
Changing RSTP bridge parameters 207
Changing RSTP port parameters 210

Chapter 23 Configuring Trunks

In this chapter 213
Adding trunks 213

Chapter 24 Configuring a Static Station

In this chapter 215
Adding a static station 215
Modifying a static station 216

Chapter 25 Configuring IP

In this chapter 219
Configuring the router IP address 219
Configuring a standard ACL 220
Configuring an extended ACL 222
Configuring an IP access group 224
Configuring an IP AS-path access list 225
Configuring an IP community list 226
Configuring an IP prefix list 228
Configuring a DNS entry 229
Configuring the general IP settings 230
Configuring IP interfaces 231
Configuring a static ARP 232
Configuring a static RARP 233

Configuring a static route 234
Configuring a UDP helper 236
Enabling forwarding for a UDP application. 237

Chapter 26 Configuring OSPF

In this chapter 239
Configuring an OSPF area 239
Configuring the OSPF area range. 240
Configuring the general OSPF settings 242
Configuring OSPF interfaces. 243
Configuring an OSPF redistribution filter 245
Configuring OSPF virtual link interfaces 247
Configuring an OSPF trap 248

Chapter 27 Configuring RIP

In this chapter 251
Configuring the general RIP settings 251
Configuring a RIP interface. 252
Configuring a RIP neighbor filter 255
Configuring a RIP route filter 256
Configuring a filter group. 257
Configuring a RIP redistribution filter 258

Chapter 28 Configuring PIM

In this chapter 261
Configuring the general PIM settings. 261
Enabling a PIM interface 262

Chapter 29 Configuring DVMRP

In this chapter 265
Configuring the general DVMRP settings 265
Configuring IGMP parameters 267
Configuring a DVMRP interface 268

Chapter 30 Configuring BGP

In this chapter 271
Configuring the general BGP settings 271
Configuring a BGP address filter 273
Configuring a BGP aggregate address. 274

Configuring a BGP AS-path filter 276
Configuring a BGP community filter 277
Configuring a BGP neighbor 278
Configuring a BGP distribute list 280
Configuring a BGP filter list 281
Configuring a BGP prefix list 282
Configuring a BGP route map 283
Configuring a BGP network 284
Configuring BGP redistribute parameters 285
Configuring a BGP route map filter 286
Configuring a route map match 288
Configuring a route map set 289

Chapter 31 Configuring a Virtual Redundant Router

In this chapter 291
Modifying a VRRP interface 291
Configuring a VRRP virtual router 292
Configuring track ports 294
Modifying a VRRP-E interface 296
Configuring a VRRP-E virtual router 296
Configuring track ports 298
Modifying a VSRP interface 299
Configuring a VSRP virtual switch 301
Configuring track ports 302

Section III Device Commands

Chapter 32 Basic Device Commands

In this chapter 307
Clearing information for a Layer 2 switch 307
Clearing information for a Layer 3 switch 308
Disabling or enabling the menu view 309
Logging out 309
Reloading units in a stack 310
Saving the configuration to flash 311
Switching over to the active role 311
Performing hitless-reload from primary images 312
Performing hitless-reload from secondary images 313
Accessing the Telnet command prompt 314
Performing a trace 315

Chapter 33 Using TFTP

In this chapter 317
Configuring TFTP 317
Configuring a TFTP image 318

About This Document

In this chapter

- Audience. xiii
- Supported hardware and software. xiii
- Document conventions xiv
- Notice to the reader xiv
- Related publications xv
- Getting technical help xv

Audience

This document is designed for system administrators with a working knowledge of Layer 2 and Layer 3 switching and routing.

If you are using a Brocade Layer 3 switch, you should be familiar with the following protocols if applicable to your network: IP, RIP, OSPF, BGP, ISIS, IGMP, PIM, and VRRP.

Supported hardware and software

This guide describes software release 07.3.00 of the Brocade FastIron CX, Brocade FastIron SX, and Brocade ICX 6610 devices.

The following hardware platforms are supported by this release of this guide:

- Brocade FastIron SX 800 (FSX 800)
- Brocade FastIron SX 1600 (FSX 1600)
- Brocade FastIron SX 1600-ANR (FSX 1600-ANR) Layer 2 or Layer 3 switches
- Brocade FCX624S
- Brocade FCX648S
- Brocade FCX624S-F
- Brocade FCX624S-HPOE
- Brocade FCX648S-HPOE
- Brocade FCX624-E
- Brocade FCX624-I

- Brocade FCX648-E
- Brocade FCX648-I
- Brocade ICX 6610

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names
	Identifies the names of user-manipulated GUI elements
	Identifies keywords
	Identifies text to enter at the GUI or CLI
italic text	Provides emphasis
	Identifies variables
	Identifies document titles

For readability, command names in the narrative portions of this guide are presented in bold: for example, **show version**.

Notes

The following notice is used in this manual.

NOTE
A note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

Notice to the reader

This document may contain references to the trademarks of the following corporations. These trademarks are the properties of their respective companies and corporations.

These references are made for informational purposes only.

Corporation	Referenced Trademarks and Products
Microsoft Corporation	Internet Explorer 6.0 and 7.0
Netscape Communications Corporation	Netscape

Corporation	Referenced Trademarks and Products
Apple Inc.	Safari 3.1
Google Inc.	Google Chrome
Mozilla Corporation	Mozilla Firefox
Opera Software ASA	Opera

Related publications

The following Brocade documents supplement the information in this guide:

- *Brocade FastIron CX Hardware Installation Guide*
- Brocade FastIron X Series Chassis Hardware Installation Guide
- Brocade ICX 6610 Stackable Switch Hardware Installation Guide
- FastIron Configuration Guide

NOTE
For the latest edition of these documents, which contain the most up-to-date information, see Product Manuals at kp.foundrynet.com.

Getting technical help

Brocade is committed to ensuring that your investment in our products remains cost-effective. If you need assistance or find errors in the manuals, contact Brocade using one of the following options.

Web access

The Knowledge Portal (KP) contains the latest version of this guide and other user guides for the product. You can also report errors on the KP.

Log in to my.Brocade.com, click the **Product Documentation** tab, then click the link to the Knowledge Portal (KP). Then click **Cases** > **Create a New Ticket** to report an error. Make sure you specify the document title in the ticket description.

E-mail and telephone access

Go to *http://www.brocade.com/services-support/index.page* for the latest e-mail and telephone contact information.

In this chapter

Chapter

1 Getting Started with the Web GUI

In this chapter

- Access requirements 1
- Logging in to the Web Management Interface 2
- Logging out of the Web Management Interface 4
- Using the Web Management Interface 4

Access requirements

The Web Management Interface is a browser-based interface that allows administrators to manage and monitor a single Brocade device or a group of Brocade devices connected together. For many of the features on a Brocade device, the Web Management Interface can be used as an alternate to the CLI for creating new configurations, modifying existing ones, and monitoring the traffic on a device.

NOTE
The Web Management Interface does not provide network management capabilities. If you need to manage a network of Brocade devices, use the IronView Network Manager or the Brocade Network Advisor application.

The Web Management Interface can be accessed from a management station using a web browser through an HTTP connection. The management options can be accessed from a menu tree or a list. The menu tree view is available when you use the Web Management Interface with the following web browsers:

- Netscape 4.0 or higher
- Internet Explorer 4.0 or higher
- Safari 3.1
- Google Chrome
- Mozilla Firefox
- Opera

For all the other older browsers, the Web Management Interface displays only the list view.

The following requirements must be met for accessing the Web Management Interface:

- A management station, such as a PC, with a web browser, that is either connected directly to the Brocade device or is on the network of the device to be managed.
- The device must have an IP address. The IP address can be assigned using the CLI. For more information on IP addresses for a device, refer to the *FastIron Configuration Guide.*
- The device must be powered on before you begin management activities.

Logging in to the Web Management Interface

To log in to the Web Management Interface, perform the following steps.

1. Open a web browser and enter the IP address of the Brocade device in the Location or Address field.

   The web browser contacts the Brocade device and displays the login page, as shown in Figure 1.

FIGURE 1 Web Management Interface login page

NOTE
If you are unable to connect with the device through a web browser due to a proxy problem, it may be necessary to set your web browser for direct Internet access instead of using a proxy. For information on how to change a proxy setting, refer to the online help provided with your web browser.

2. Click **Login**. The dialog box as shown Figure 2 is displayed.

FIGURE 2 User name and password dialog box

3. Perform one of the following procedures:

- For read-only access, enter the user name as **get** and a read-only community string for the password. The community string **public** is the default read-only community string.
- For read-write access, enter the user name as **set** and a read-write community string for the password. There is no default read-write community string.

NOTE
If you have configured the device to secure the Web Management Interface using local user accounts, you must enter the user name and password of one of the user accounts.

Figure 3 displays the home page of the Web Management Interface for a Layer 2 switch.

FIGURE 3 Home page for Layer 2 switch features

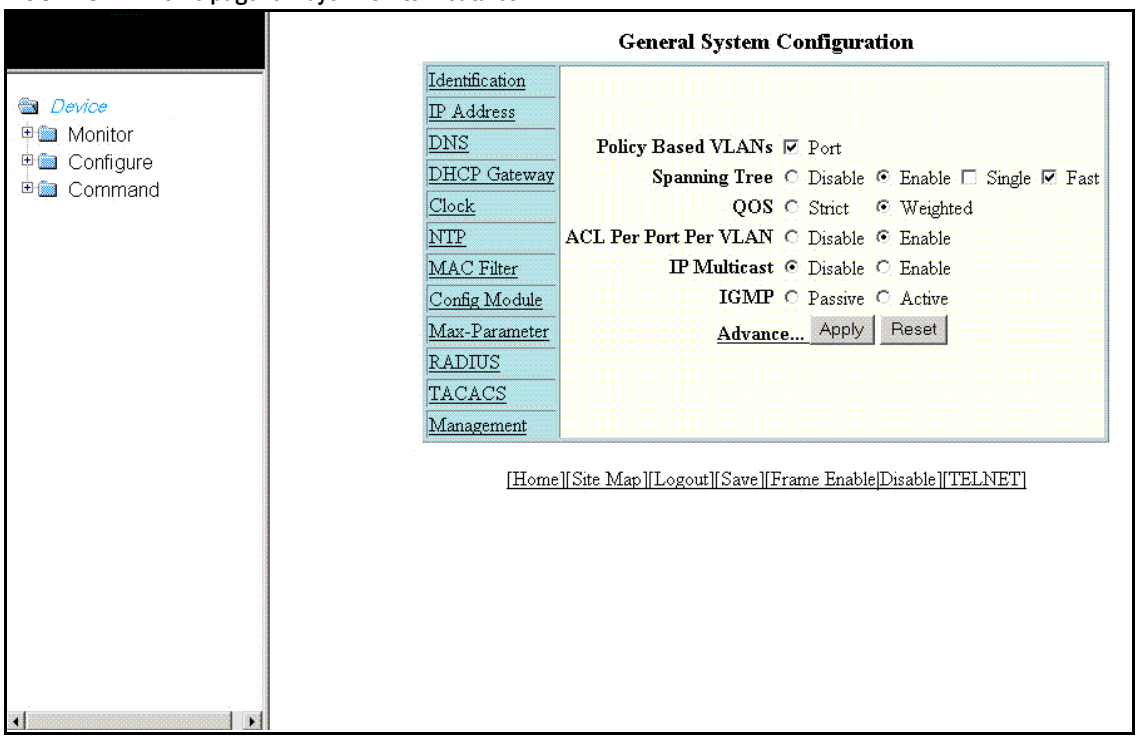
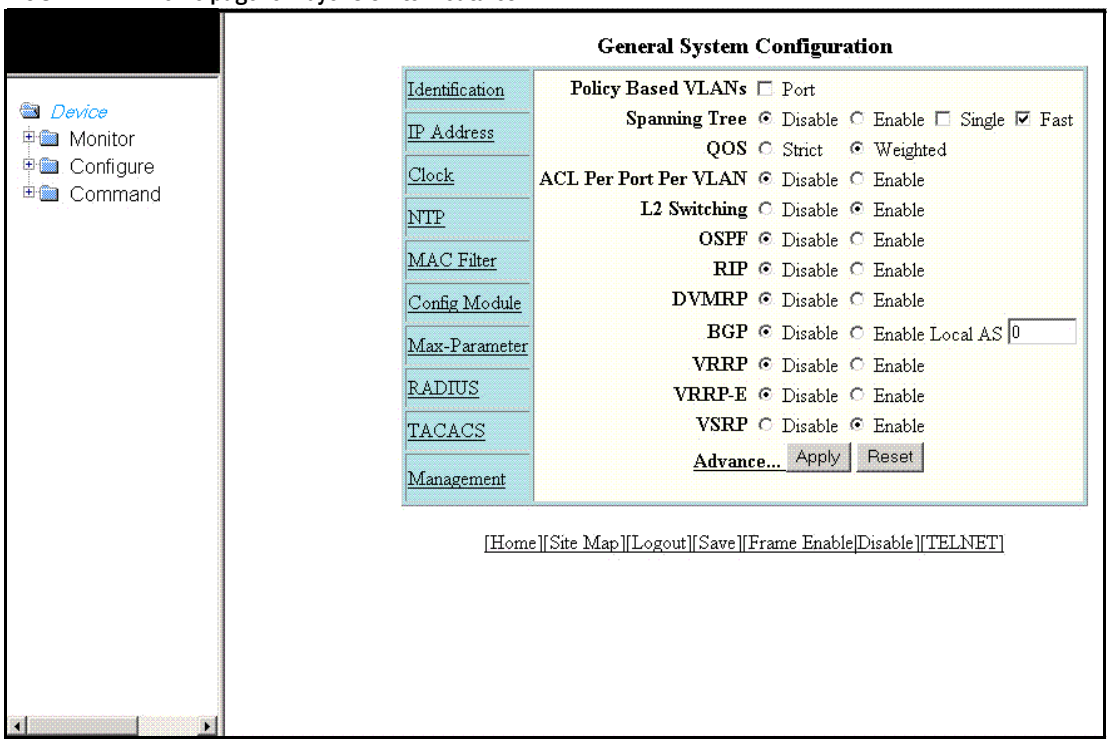


Figure 4 displays the home page of the Web Management Interface for a Layer 3 switch.

FIGURE 4 Home page for Layer 3 switch features



NOTE
If you are using Internet Explorer 6.0 to view the Web Management Interface, make sure the version you are running includes the latest service packs. Otherwise, the navigation tree (the left-most pane in Figure 3 and Figure 4) will not display properly. For information on how to load the latest service packs, refer to the online help provided with your web browser.

Logging out of the Web Management Interface

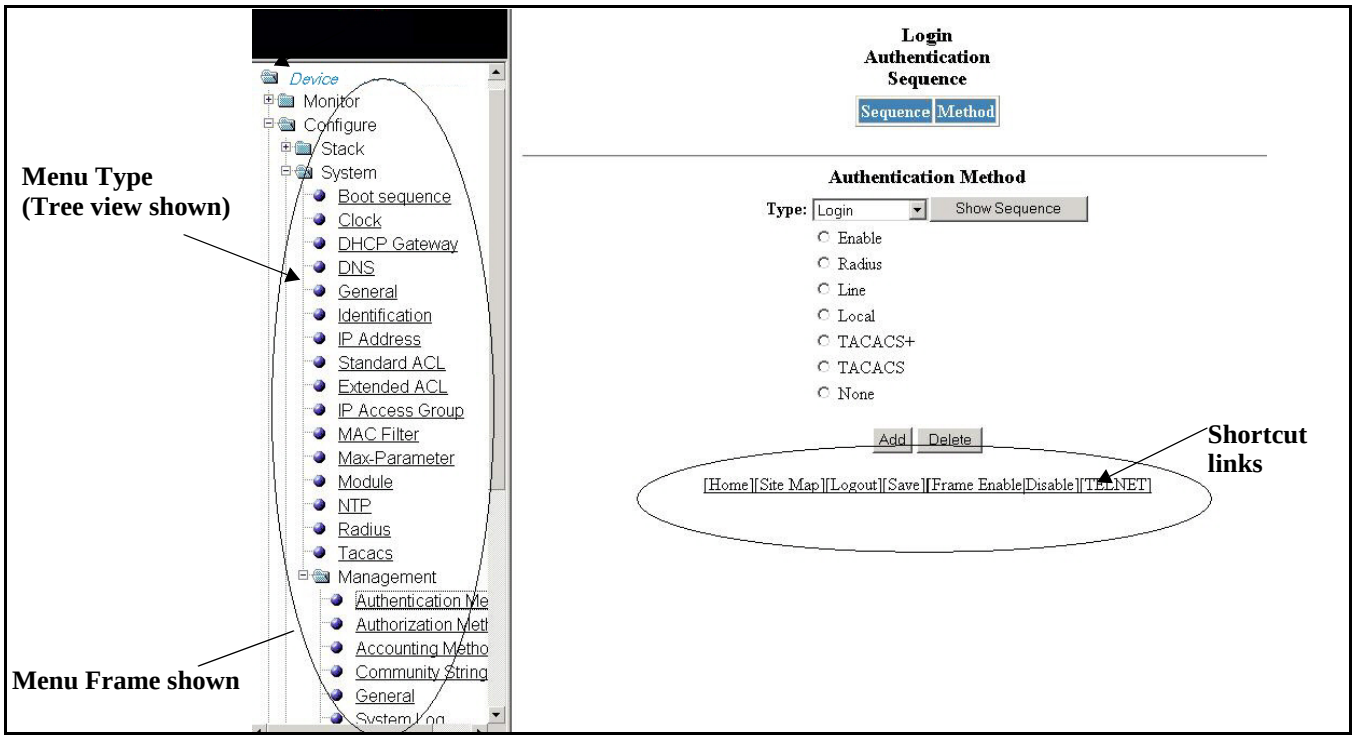
You can log out of the Web Management Interface in two ways:

- Click **Logout** on the window.
- Click **Command** in the left pane and select **Logout**.

Using the Web Management Interface

The following procedure explains in detail about using the Web Management Interface.

1. Click the plus sign (+) next to **Configure** in the tree view to expand the list of configuration options.
2. Click the plus sign (+) next to **System** in the tree view to expand the list of system configuration links.
3. Click the plus sign (+) next to **Management** in the tree view to expand the list of system management links.
4. Click **Authentication Methods** to display the **Authentication Method** panel.
5. Enable or disable elements on the Web Management Interface by clicking the appropriate options on the panel. The following illustration identifies the elements you can change.



NOTE
The tree view is available when you use the Web Management Interface with Netscape 4.0 or higher or Internet Explorer 4.0 or higher. If you use the Web Management Interface with an older browser, the Web Management Interface displays the list view only, and the Web Management Preferences panel does not include an option to display the tree view.

6. When you have finished, click **Add** on the panel to add the authentication types. Click **Delete** to remove authentication types.
7. To save the configuration, click the plus sign (+) next to the **Command** folder, and then click **Save to Flash**.

NOTE
The only changes that become permanent are the settings to the Menu Type and the Front Panel Frame. Any other elements you enable or disable will go back to their default settings the next time you start the Web Management Interface.

Web Management Interface areas

The following sections describe the Web Management Interface areas and how to use them.

Menu tree or list

The left panel shows the menu tree or list of options. The interface can be set up to display a menu tree or a list of options. You can enable or disable the menu tree view in two ways:

- Click **Frame Enable|Disable** on the bottom of the window.
- Click **Command** and select **Disable Frame**.

Configuration panel

The configuration panel consists of the tables with the field elements that display information or the input fields for which the values have to be entered. The input fields can be of four types:

- Fields into which data must be entered using the keyboard.
- Lists from which one of several options can be chosen.
- Options allow you to select only one of the settings or features of a set of options.
- Check boxes allow you to turn on or off a parameter and you can also make multiple selections.

After entering the values, you must click the appropriate button to configure the values.

Shortcuts to functions and other panels

All the pages in the Web Management Interface provide shortcut links to the functions that are specific to that page and to other panels. All of the Web Management Interface panels have the following links:

- **[Home]** – Returns you to the home page of the Web Management Interface.
- **[Site Map]** – Lists all options available from the Web Management Interface with links to the panels for those options. Use the **Site Map** link to move through the interface if the menu is not displayed.
- **[Logout]** – Logs you out of the Web Management Interface.
- **[Save]** – Saves the changes you entered on the panels.
- **[TELNET]** – Opens a Telnet session to the device.
- **[Frame Enable|Disable]** – Enables or disables the bookmark options available in the left panel. If frames are disabled, you will not be able to choose any of the options on the web preference panel that use frames.

Section

I

Monitoring Device Performance and Metric

This section describes the **Monitor** features, and includes the following chapters:

- Monitoring Basic Device Information 9
- Monitoring Stacks 25
- Monitoring Ports 35
- Monitoring STP. 51
- Monitoring RSTP 55
- Monitoring IP 59
- Monitoring OSPF 69
- Monitoring PIM. 89
- Monitoring DVMRP 93
- Monitoring BGP 99
- Monitoring Virtual Redundant Router 107
- Monitoring RMON 115

Chapter

Monitoring Basic Device Information

2

In this chapter

- Displaying the ARP cache 9
- Displaying the device information 10
- Displaying flash information 13
- Displaying memory information 13
- Displaying the front panel 14
- Displaying MAC addresses 20
- Displaying the system log 21

Displaying the ARP cache

The Address Resolution Protocol (ARP) cache table contains entries that map IP addresses to Media Access Control (MAC) addresses. There are two types of ARP entries: static (user-configured) and dynamic (learned).

To display the ARP cache information, click **Monitor** on the left pane and select **ARP Cache.**

The **ARP Cache** window is displayed as shown in Figure 5.

FIGURE 5 Monitoring the ARP cache

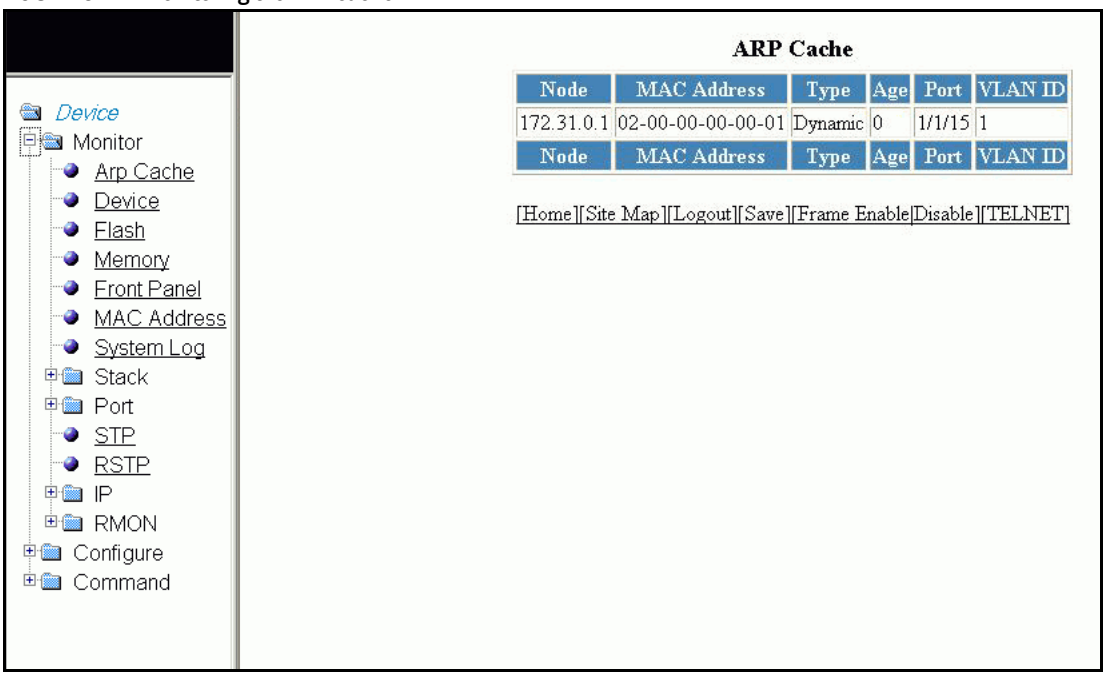


Table 1 describes the fields in the **ARP Cache** window.

TABLE 1 Description of the fields in the **ARP Cache** window

Field	Description
Node	Displays the IP address of the device.
MAC Address	Displays the MAC address of the device.
Type	Displays the type of ARP entry, which can be one of the following: • **Dynamic** – The Layer 3 switch learned the entry from an incoming packet. • **Static** – The Layer 3 switch loaded the entry from the static ARP table when the device for the entry was connected to the Layer 3 switch.
Age	Displays the number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the cache. **NOTE:** Static entries do not age out.
Port	Displays the port attached to the device for which the entry was made. For dynamic entries, this is the port on which the entry was learned. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
VLAN ID	Displays the VLAN Identifier of the port, which learned the entry. **NOTE:** This field is not available in the **ARP Cache** window for the Brocade FSX devices.

Displaying the device information

To display the device information, perform the following steps.

1. Click **Monitor** on the left pane and select **Device**.
2. For Brocade FCX and Brocade ICX 6610 devices, select a stack Identifier from the **Stack Unit ID** list and click **Display** to view the information for any device in an IronStack.

NOTE
The **Stack Unit ID** list is not available in the **Device Information** window for the Brocade FSX devices.

The **Device Information** window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 6.

FIGURE 6 Monitoring the device information

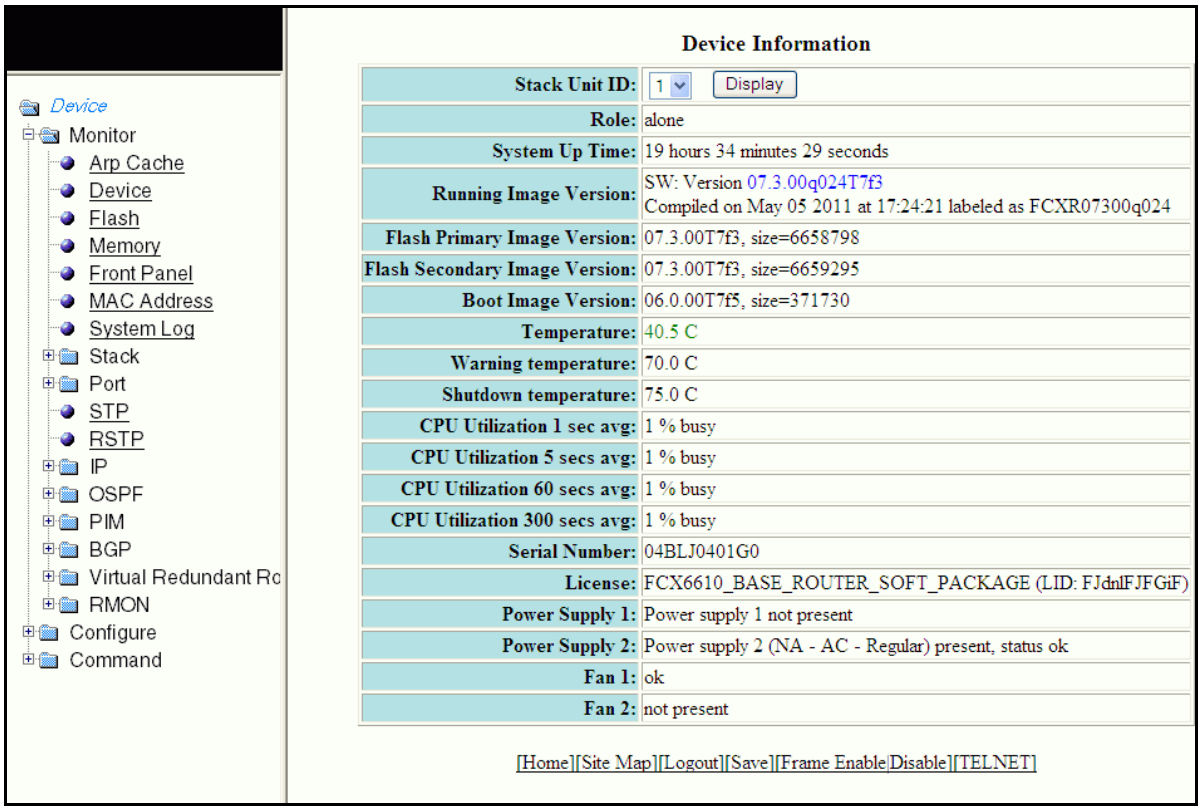


Table 2 describes the fields in the **Device Information** window.

TABLE 2 Description of the fields in the **Device Information** window

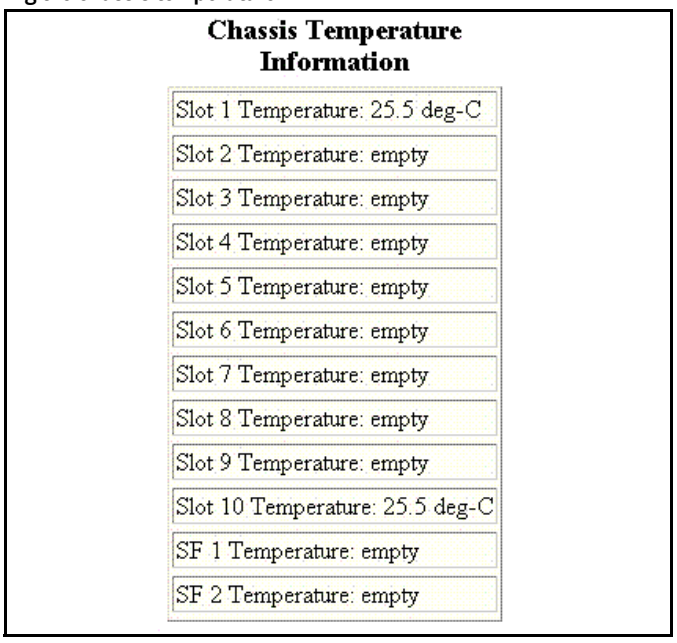
Field	Description
Stack Unit ID	Displays the number of the unit within a stack from 1 through 8. **NOTE:** This field is not available in the **Device Information** window for the Brocade FSX devices.
Role	Displays the role of the device, which can be **Active**, **Standby**, **Member**, or **alone**. If the role is **alone**, the device is operating as a standalone device. **NOTE:** This field is not available in the **Device Information** window for the Brocade FSX devices.
System Up Time	Displays the quantity of time the system has been running since the last restart.
Running Image Version	Displays the software version currently running and some details on the version.
Flash Primary Image Version	Displays the release number and size of the software loaded on the primary flash.
Flash Secondary Image Version	Displays the release number and size of the software loaded on the secondary flash.
Boot Image Version	Displays the release number and size of the boot image.

TABLE 2 Description of the fields in the **Device Information** window (Continued)

Field	Description
Temperature	For Brocade FCX and Brocade ICX 6610 devices, this field displays the actual temperature. The color of the degrees provides a visual indicator for the device: • Green – The temperature is within the normal operating range. • Orange – The temperature has reached the warning level. • Red – The temperature has reached the shutdown level. For Brocade FSX devices, click **Temperature** in the right pane to display the **Chassis Temperature Information** window, which shows the temperature of each slot from 1 through 10 and the switch fabric modules SF 1 and SF 2. Figure 7 shows the **Chassis Temperature Information** window.
Warning temperature	Displays the warning level temperature. **NOTE:** This field is not available in the **Device Information** window for Brocade FSX devices.
Shutdown temperature	Displays the shutdown level temperature. **NOTE:** This field is not available in the **Device Information** window for Brocade FSX devices.
CPU Utilization	Displays the percentage of Central Processing Unit (CPU) being used by the device.
Serial Number	Displays the serial number of the device.
License	Displays the software license and License ID (LID) of the device. **NOTE:** This field is not available in the **Device Information** window for Brocade FSX devices.
Power Supply 1	Displays the status of the primary power supply.
Power Supply 2	Displays the status of the secondary power supply, if present.
Fan	Displays the status of the cooling fans. **NOTE:** There is an entry for each fan in the device.

Figure 7 shows the **Chassis Temperature Information** window.

FIGURE 7 Monitoring the chassis temperature


Chassis Temperature Information
Slot 1 Temperature: 25.5 deg-C
Slot 2 Temperature: empty
Slot 3 Temperature: empty
Slot 4 Temperature: empty
Slot 5 Temperature: empty
Slot 6 Temperature: empty
Slot 7 Temperature: empty
Slot 8 Temperature: empty
Slot 9 Temperature: empty
Slot 10 Temperature: 25.5 deg-C
SF 1 Temperature: empty
SF 2 Temperature: empty

Displaying flash information

NOTE
This feature is applicable only for the Brocade FCX and Brocade ICX 6610 devices.

To display the flash information, click **Monitor** on the left pane and select **Flash.**

The **Flash Information** window is displayed as shown in Figure 8.

FIGURE 8 Monitoring the flash information

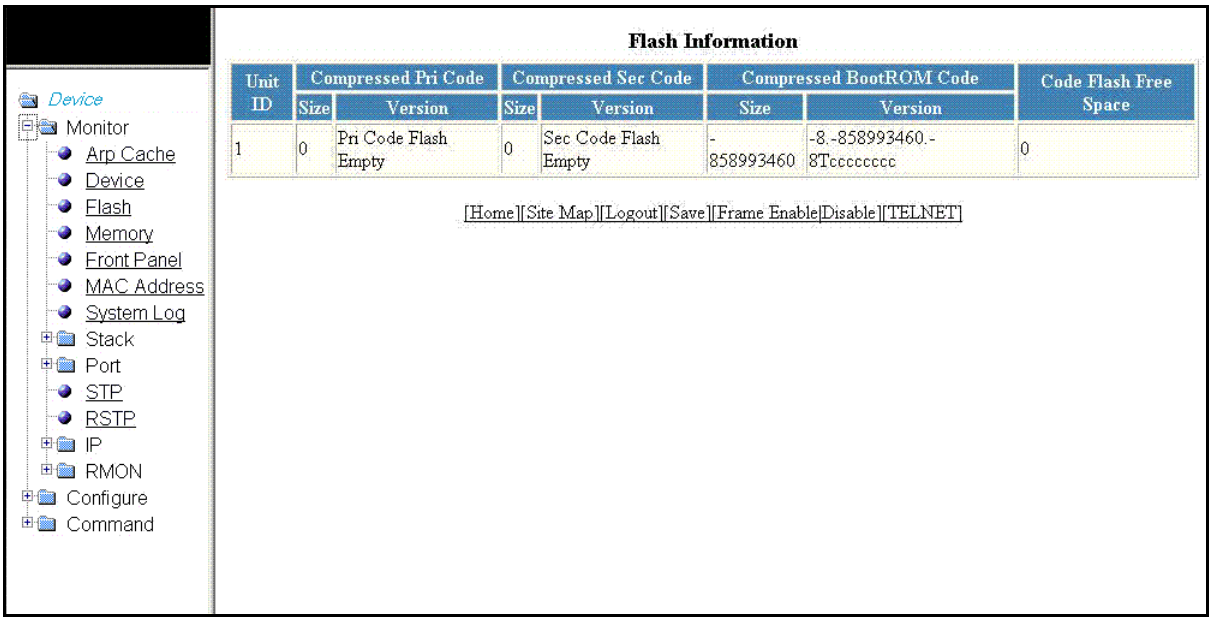


Table 3 describes the fields in the **Flash Information** window.

TABLE 3 Description of the fields in the **Flash Information** window

Field	Description
Unit ID	Displays the number of the unit within a stack from 1 through 8.
Compressed Pri Code	Displays the compressed size and version for the primary code.
Compressed Sec Code	Displays the compressed size and version for the secondary code.
Compressed BootROM Code	Displays the compressed size and version for the BootROM code.
Code Flash Free Space	Displays the amount of free space available on the flash memory.

Displaying memory information

NOTE
This feature is applicable only for the Brocade FCX and Brocade ICX 6610 devices.

To display the memory information of the device, click **Monitor** on the left pane and select **Memory.**

The **Memory Information** window is displayed as shown in Figure 9.

FIGURE 9 **Monitoring the memory information**

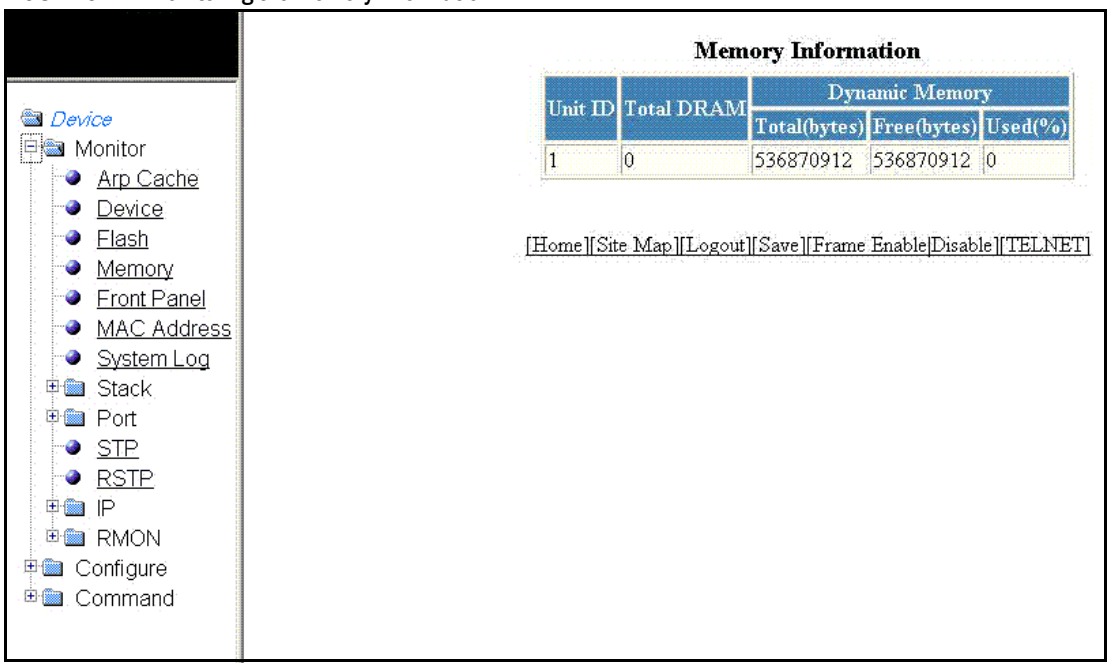


Table 4 describes the fields in the **Memory Information** window.

TABLE 4 Description of the fields in the **Memory Information** window

Field	Description
Unit ID	Displays the number of the unit within a stack from 1 through 8.
Total DRAM	Displays the size (in bytes) of dynamic random access memory (DRAM).
Dynamic Memory	Displays the total number of bytes in dynamic memory, including the number of bytes that are available (free or unused), and the percentage of memory used.

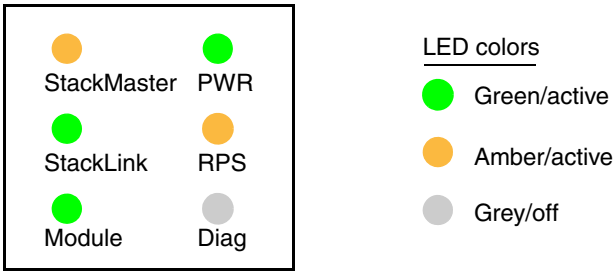
Displaying the front panel

The front panel of the device allows you to view the modules in each device and the ports within each module.

The front panel shows the status of devices using colors. Green ports are connected, and gray ports are not connected. Ports of the same color on two units are connected with cables. A gray uplink port is not connected to a device.

Status LED display

The status LEDs that appear on the front panel provide information about system activity.



The following table describes the meanings of the different colors of the LEDs.

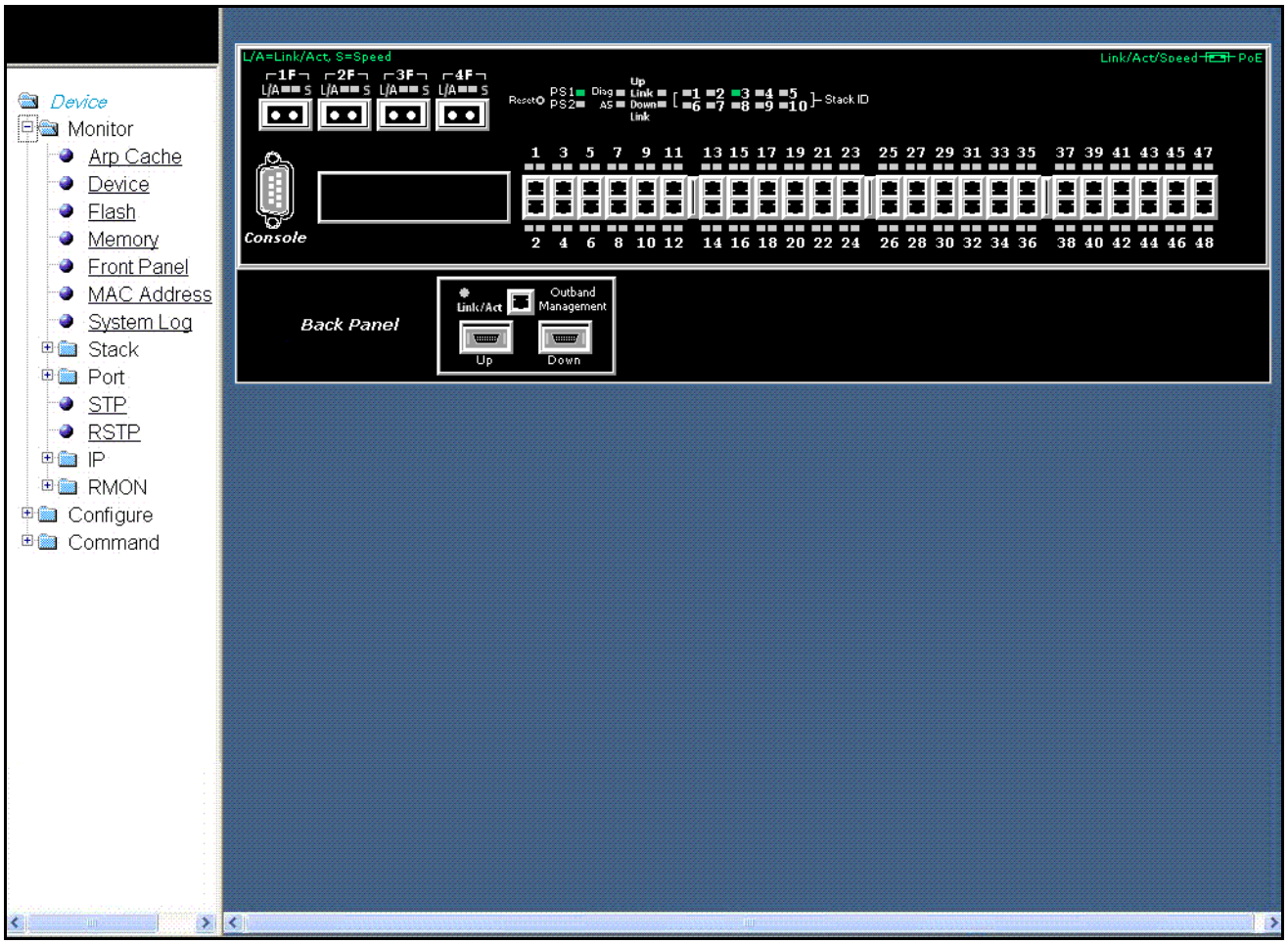
Active Controller (Device role in the stack)	• Green – Active Controller. • Amber – Standby Controller. • Off – Stack Member.
StackLink	• Green – Both stacking physical links are active. • Amber – One stacking physical link is active. • Off – None of the stacking ports are active.
Module	• Green – Both stacking 10 Gb modules are present. • Amber – One stacking 10 Gb module is present. • Off – No stacking 10 Gb module.
PWR (Power)	• Green – Power is on. • Amber - Power supply failure. • Off – Power is off.
RPS (Redundant Power Supply)	• Green – RPS is operational (the main supply power is unplugged). • Amber – RPS is on standby (the main supply power is on). • Off – RPS is not plugged in.
Diag (Diagnostics)	• Green – Manufacturing diagnostics are in progress. • Off – No manufacturing diagnostics.

Displaying the front panel for Brocade FCX devices

To display the front panel, click **Monitor** on the left pane and select **Front Panel**.

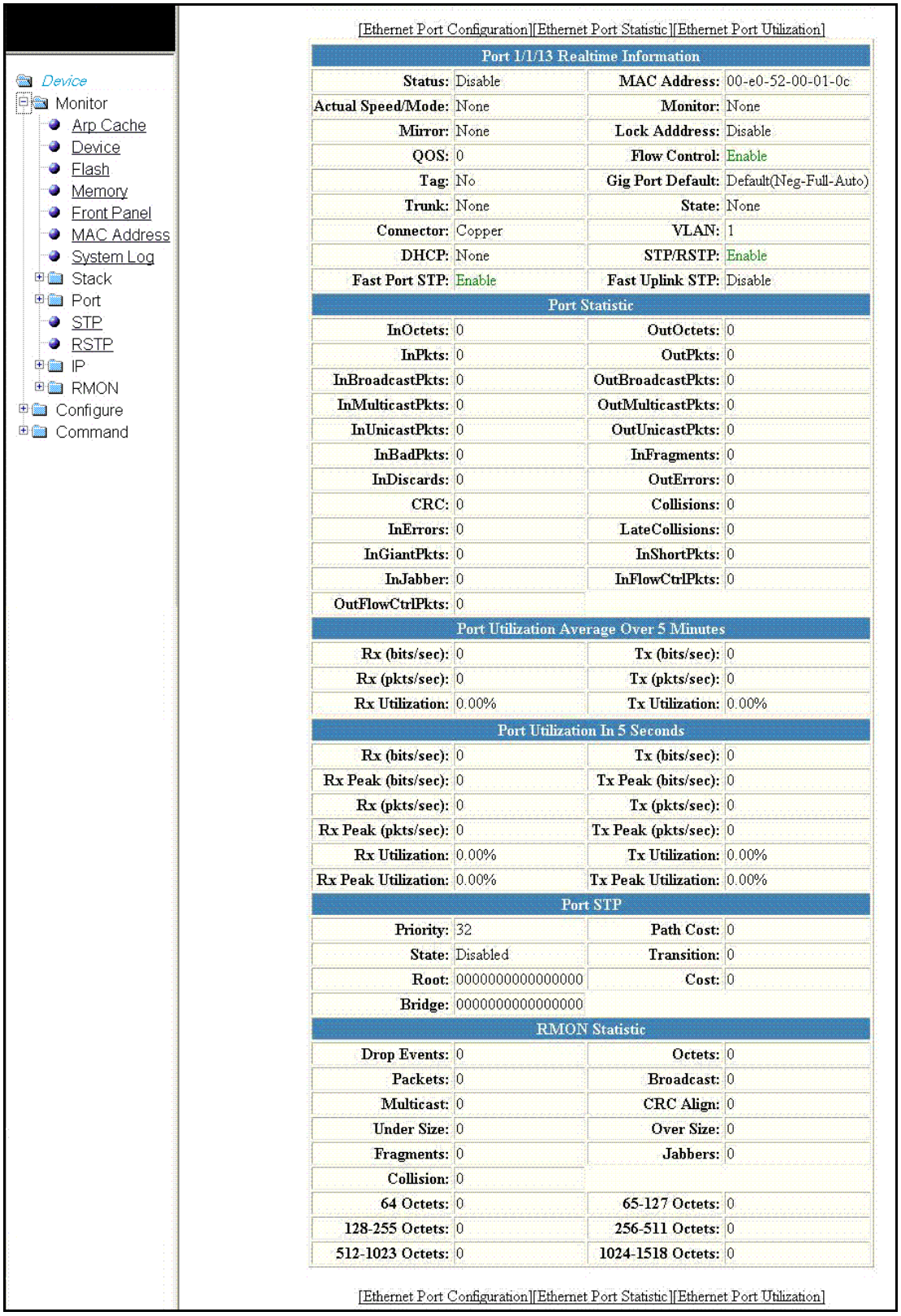
Figure 10 shows the front panel for the Brocade FCX648 device.

FIGURE 10 Brocade FCX648 front panel



Click any port to display the real-time port information for that port. Figure 11 shows the **Port Realtime Information** window. Clicking elsewhere on the panel opens the **Device Information** window. For more information, refer to "Displaying the device information" on page 10.

FIGURE 11 Monitoring the real-time port information for FCX devices



The **Port Realtime Information** window provides links to configure and monitor port parameters:

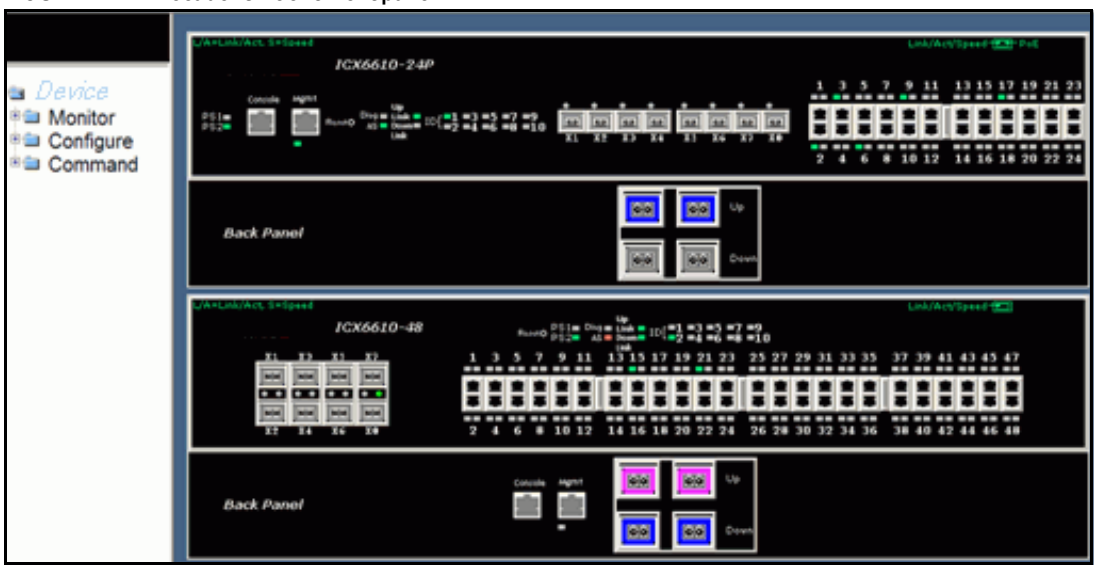
- To configure an Ethernet port, click **Ethernet Port Configuration**. For more information, refer to "Configuring an Ethernet port" on page 175.
- To view the total number of packets, number of collisions, and number of errors that have occurred on a port, click **Ethernet Port Statistic**. For more information, refer to "Displaying Ethernet port statistics" on page 35.
- To view the traffic that is received and transmitted on a port, click **Ethernet Port Utilization**. For more information, refer to "Displaying Ethernet port utilization" on page 39.

Displaying the front panel for the Brocade ICX 6610 device

To display the front panel, click **Monitor** on the left pane and select **Front Panel**.

Figure 12 shows the front panel for the Brocade ICX 6610 device.

FIGURE 12 Brocade ICX 6610 front panel



You can perform the following tasks in the panel:

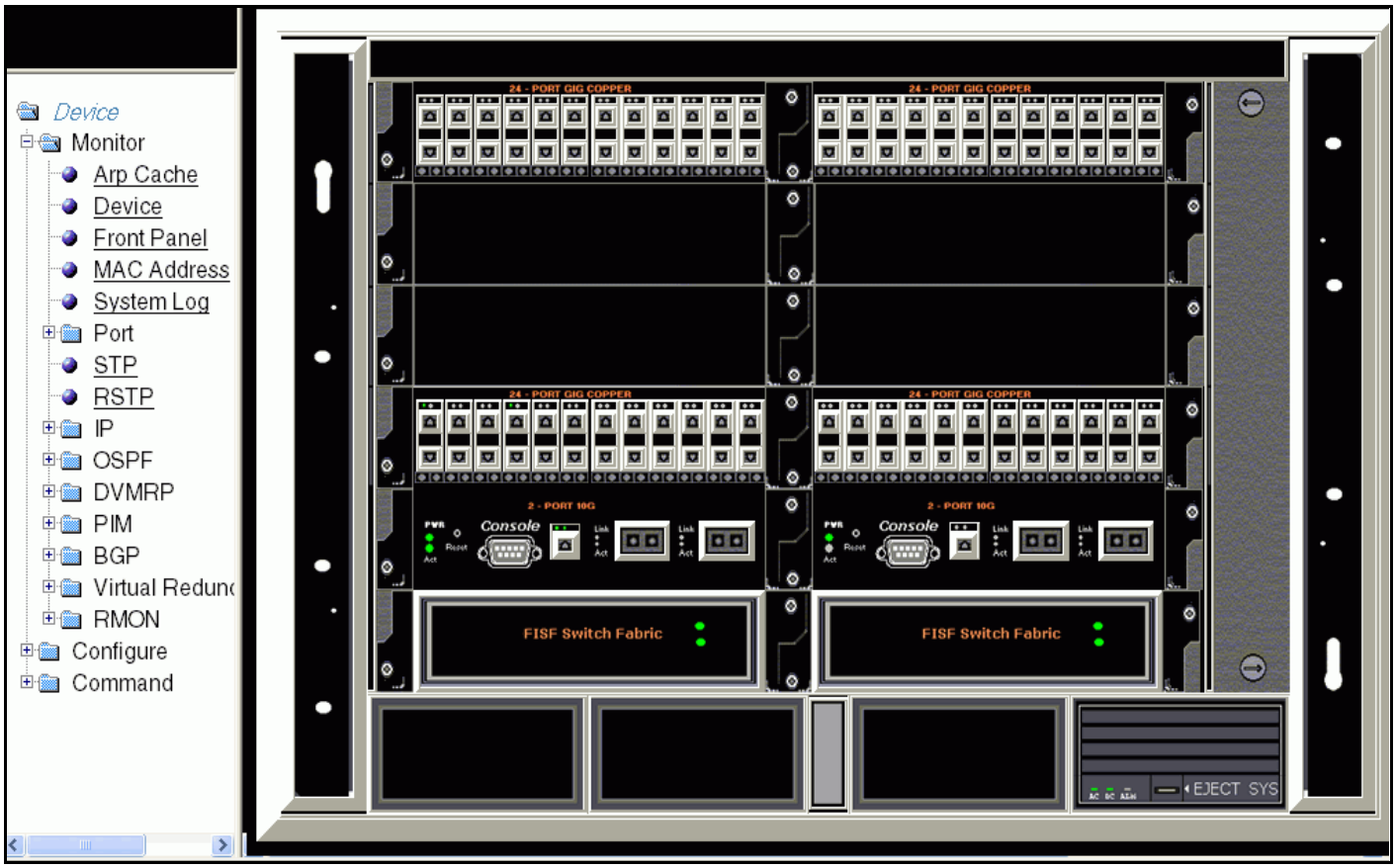
- Click **Console** port to display the device information. For more information, refer to "Displaying the device information" on page 10.
- Click **Mgmt** port to display the current management port configuration information. For more information, refer to "Displaying the management port information" on page 41.
- Click any port to display the real-time port information for that port. Figure 11 shows the **Port Realtime Information** window.
- Click elsewhere on the panel to display the **Device Information** window.

Displaying the front panel for Brocade FSX devices

To display the front panel, click **Monitor** on the left pane and select **Front Panel**.

Figure 13 shows the front panel for a Brocade FSX device.

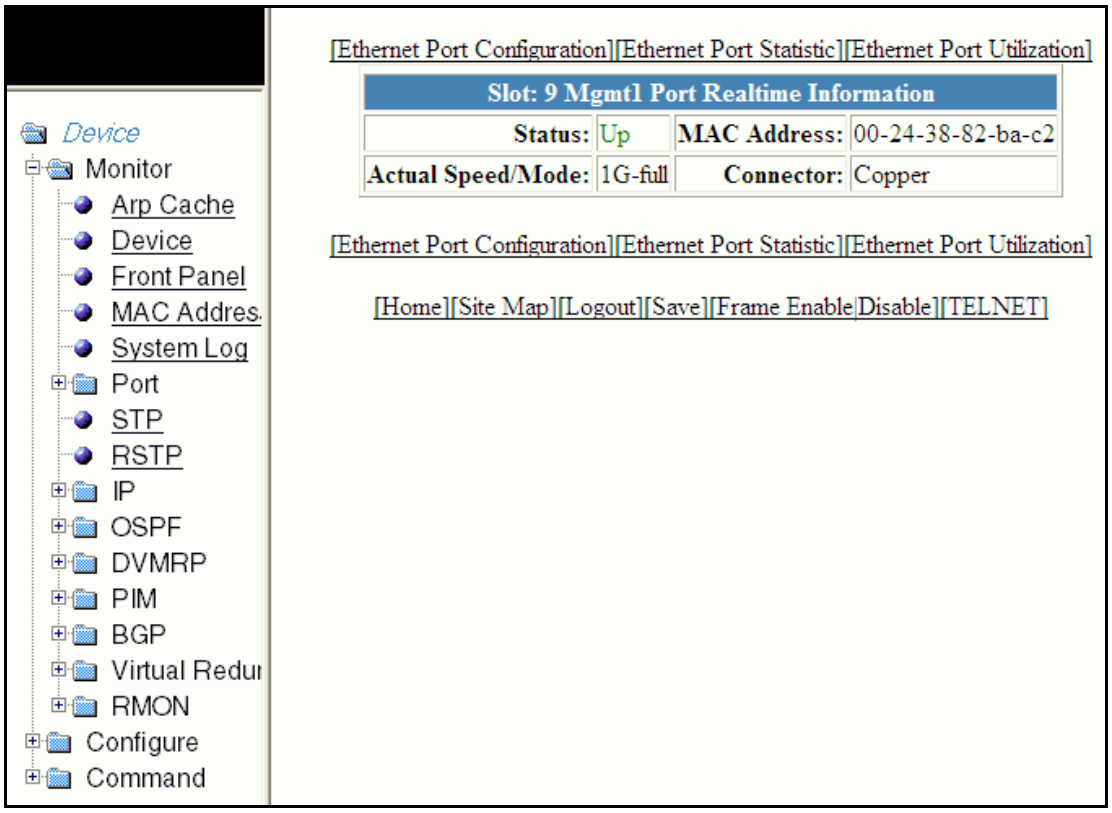
FIGURE 13 Brocade FSX front panel



You can perform the following tasks in the panel:

- Click **Console** port to display the **Device Information** window. For more information, refer to "Displaying the device information" on page 10.
- Click management port to display the current management port real-time information. Figure 14 shows the **mgmt1 Port Realtime Information** window. For more information, refer to "Displaying the management port information" on page 41.
- Click any port to display the real-time port information for that port. Figure 11 shows the **Port Realtime Information** window.
- Click elsewhere on the panel to display the **Device Information** window.

FIGURE 14 Monitoring the real-time port information of the management port



Displaying MAC addresses

To display the list of MAC addresses that have been learned by the device, click **Monitor** on the left pane and select **MAC Address**.

The **MAC Address** window is displayed as shown in Figure 15.

FIGURE 15 Monitoring the MAC address

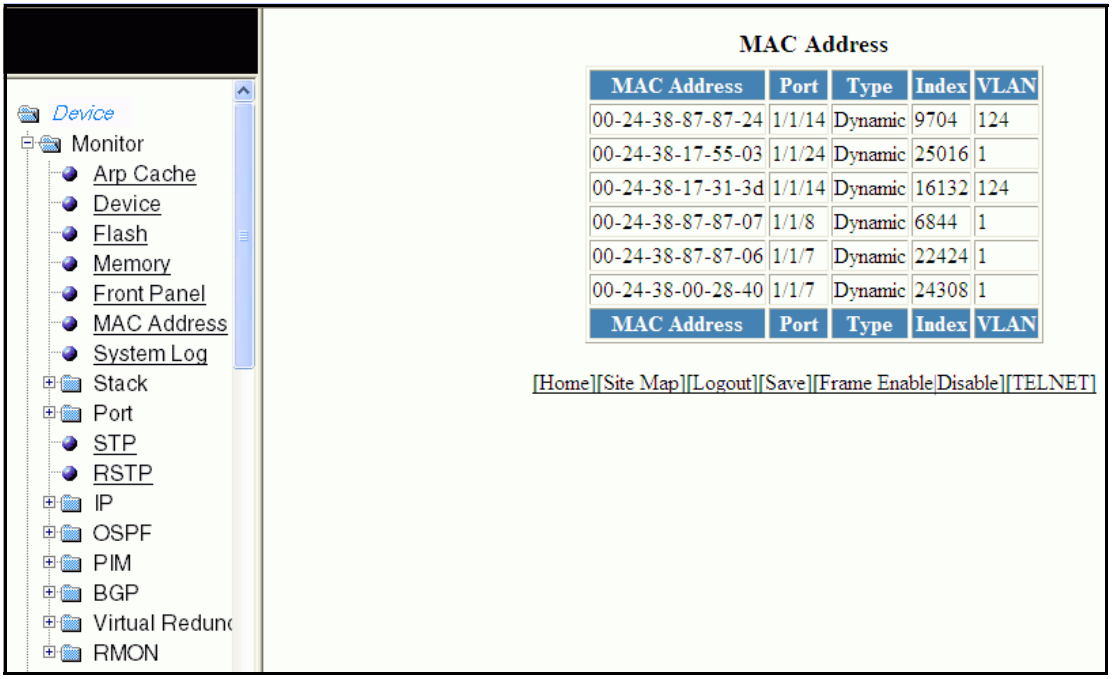


Table 5 describes the fields in the **MAC Address** window.

TABLE 5 Description of the fields in the **MAC Address** window

Field	Description
MAC Address	Displays the MAC address of the device.
Port	Displays the port attached to the device for which the entry was made. For dynamic entries, this is the port on which the entry was learned. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Type	Displays the type of the entry, which can be one of the following: • **Dynamic** – The MAC address changes if the Active Controller changes. • **Static** – The MAC address will not change if the Active Controller changes.
Index	Displays the index of the entry in the MAC Address table.
VLAN	Displays the port-based VLAN that contains this (instance of) spanning tree. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1.

Displaying the system log

The software provides two types of system log buffers:

- Static – Logs power supply failures, fan failures, and temperature warning or shutdown messages.
- Dynamic – Logs all other message types.

To display the current information of the system log buffer, click **Monitor** on the left pane and select **System Log**.

The **Dynamic System Log Buffer** window is displayed as shown in Figure 16.

FIGURE 16 Monitoring the dynamic system log buffer

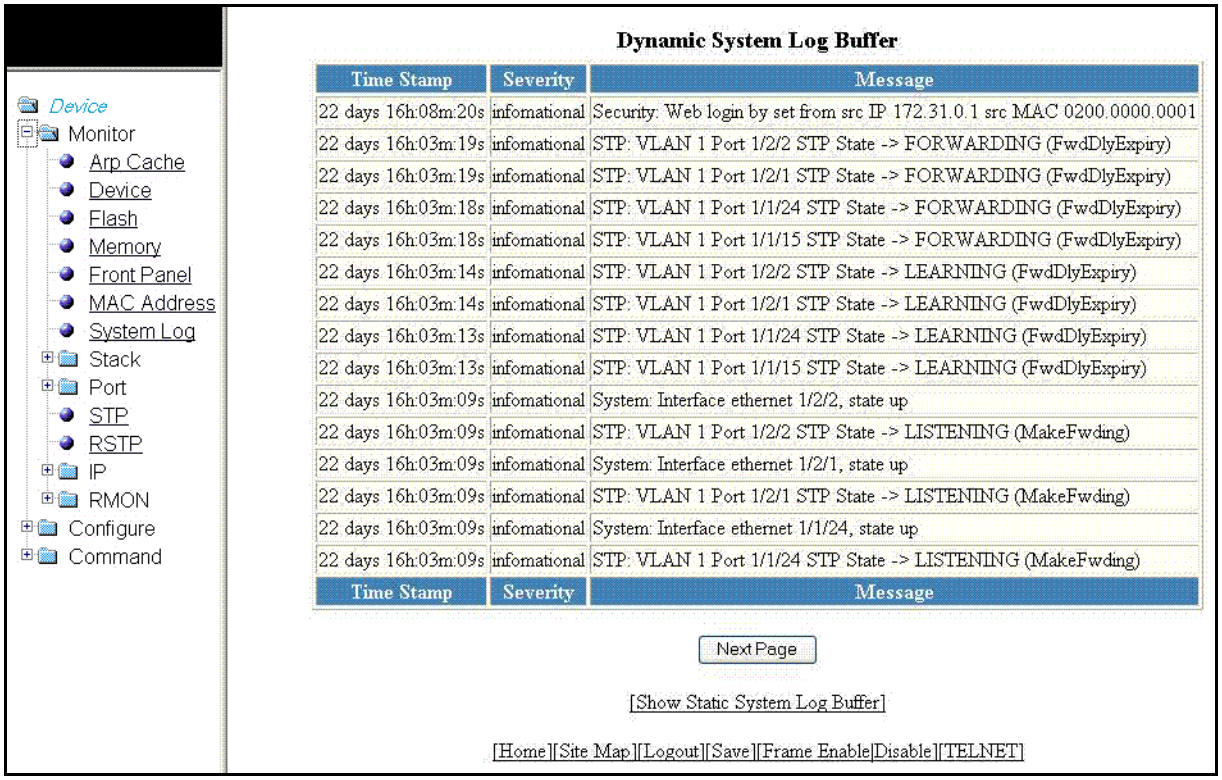

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Address
System Log
Stack
Port
STP
RSTP
IP
RMON
Configure
Command
Dynamic System Log Buffer
Time Stamp
Severity
Message
22 days 16h:08m:20s infomational Security: Web login by set from src IP 172.31.0.1 src MAC 0200.0000.0001
22 days 16h:03m:19s infomational STP: VLAN 1 Port 1/2/2 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:19s infomational STP: VLAN 1 Port 1/2/1 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:18s infomational STP: VLAN 1 Port 1/1/24 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:18s infomational STP: VLAN 1 Port 1/1/15 STP State -> FORWARDING (FwdDlyExpiry)
22 days 16h:03m:14s infomational STP: VLAN 1 Port 1/2/2 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:14s infomational STP: VLAN 1 Port 1/2/1 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:13s infomational STP: VLAN 1 Port 1/1/24 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:13s infomational STP: VLAN 1 Port 1/1/15 STP State -> LEARNING (FwdDlyExpiry)
22 days 16h:03m:09s infomational System: Interface ethernet 1/2/2, state up
22 days 16h:03m:09s infomational STP: VLAN 1 Port 1/2/2 STP State -> LISTENING (MakeFwding)
22 days 16h:03m:09s infomational System: Interface ethernet 1/2/1, state up
22 days 16h:03m:09s infomational STP: VLAN 1 Port 1/2/1 STP State -> LISTENING (MakeFwding)
22 days 16h:03m:09s infomational System: Interface ethernet 1/1/24, state up
22 days 16h:03m:09s infomational STP: VLAN 1 Port 1/1/24 STP State -> LISTENING (MakeFwding)
Time Stamp
Severity
Message
Next Page
[Show Static System Log Buffer]
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 6 describes the fields in the **Dynamic System Log Buffer** window.

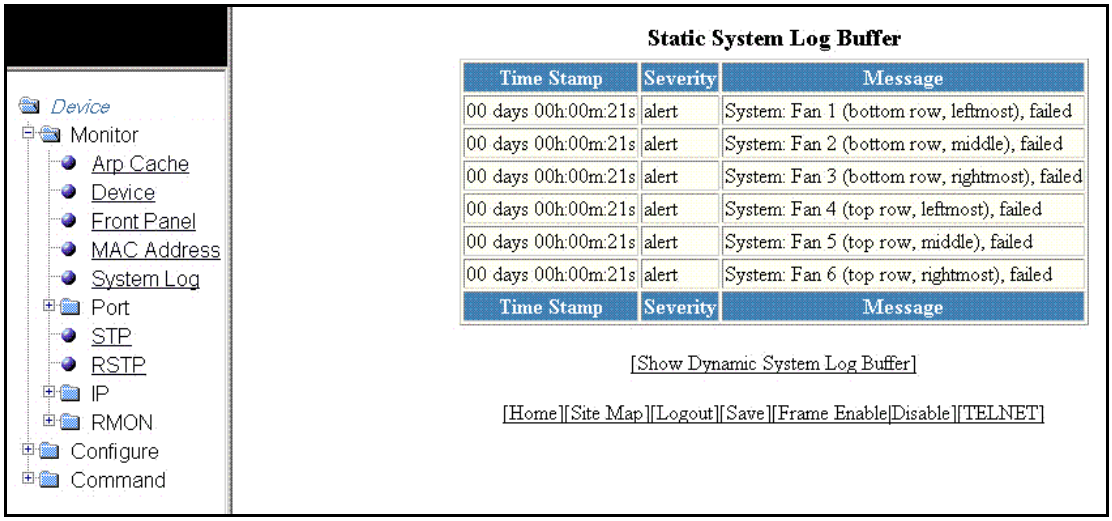
TABLE 6 Description of the fields in the Dynamic System Log Buffer window

Field	Description
Time Stamp	Displays the system uptime in DD:HH:MM:SS or the actual time if the date and time was set.
Severity	Displays the severity of the event.
Message	Displays the description of the event.

To view the next set of the **Dynamic System Log Buffer** entries, click **Next Page.** To display the static system log buffer information, click **Show Static System Log Buffer.**

The **Static System Log Buffer** window is displayed as shown in Figure 17.

FIGURE 17 Monitoring the static system log buffer



For information on the **Static System Log Buffer** fields, refer to Table 6.

Chapter

3

Monitoring Stacks

In this chapter

- Displaying the stack details 25
- Displaying a stack module 27
- Displaying stack neighbors 28
- Displaying stack ports information 29
- Displaying stack port statistics 30
- Displaying stack port interfaces 31
- Displaying stack resources 32

NOTE
This chapter is specific to Brocade FCX and Brocade ICX 6610 devices only.

Displaying the stack details

To display current stack details, stack port status, and stack neighbors information, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Details**.

The **Stack Details** window is displayed as shown in Figure 18.

FIGURE 18 Monitoring stack details

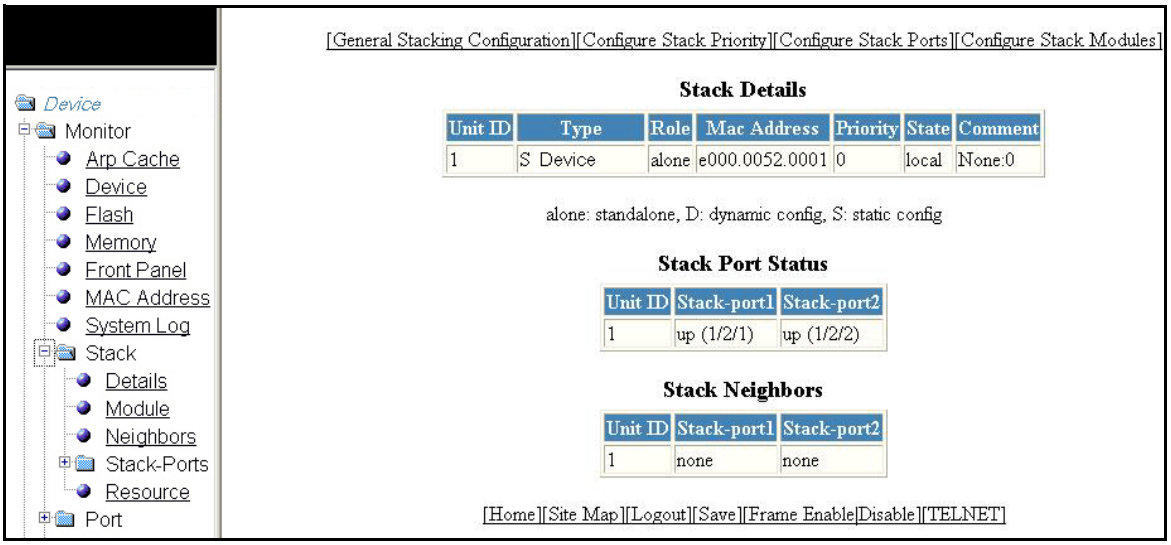


Table 7 describes the fields in the **Stack Details** window.

TABLE 7 Description of the fields in the **Stack Details** window

Field	Description
Stack Details parameters	
Unit ID	Displays the number of the unit within a stack from 1 through 8.
Type	Displays the type of configuration and the device model. The types of configuration are as follows: • **alone** – Indicates that the device is operating as a standalone device. • **S** – Indicates that the configuration for this unit is static. • **D** – Indicates that the configuration for this unit is dynamic and may be overwritten by a new stack unit.
Role	Displays the role of this unit within the stack: **Active**, **Standby**, **Member**, or **alone**.
Mac Address	Displays the MAC address of the device.
Priority	Displays the priority assigned to this unit.
State	Displays the operational state of this unit: **local** or **remote**.
Comment	Displays additional information about this unit.
Stack Port Status parameters	
Unit ID	Displays the number of the unit within a stack from 1 through 8.
Stack-port1	Displays the port state and the port number for stack-port1. The port states are as follows: • **up** – Each end is connected. • **down** – Port is configured as a stacking port, but not connected. • **none** – Port is not configured as a stacking port.
Stack-port2	Displays the port state and the port number for stack-port2. The port states are as follows: • **up** – Each end is connected. • **down** – Port is configured as a stacking port, but not connected. • **none** – Port is not configured as a stacking port.
Stack Neighbors parameters	
Unit ID	Displays the number of the unit within a stack from 1 through 8.
Stack-port1	Displays the neighbor stack unit for stack-port1 for this unit ID.
Stack-port2	Displays the neighbor stack unit for stack-port2 for this unit ID.

The **Stack Details** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Displaying a stack module

To display current information about the stack unit modules, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Module**.

The **Stack Modules** window is displayed as shown in Figure 19.

FIGURE 19 Monitor stack modules

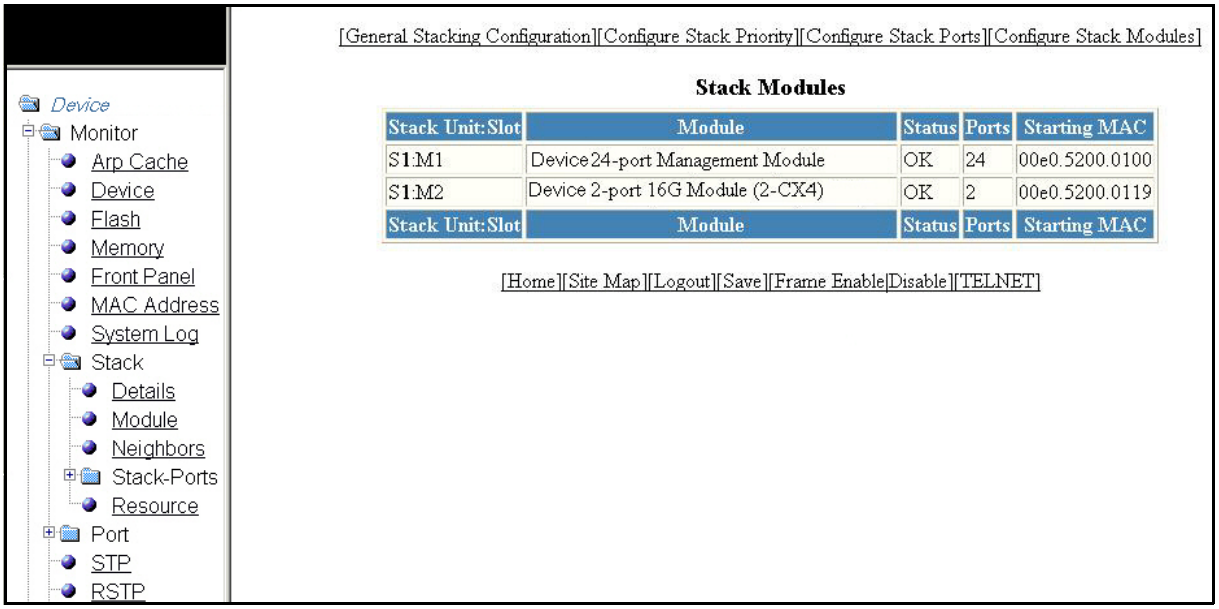


Table 8 describes the fields in the **Stack Modules** window.

TABLE 8 Description of the fields in the Stack Modules window

Field	Description
Stack Unit: Slot	Displays the number of the unit within the stack and the slot number.
Module	Displays the device information, such as module number and module type.
Status	Displays the status, which can be one of the following: • **OK** – The module came up and is operating normally. • **CFG** – The module is configured, but does not physically exist within the units of the stack.
Ports	Displays the number of ports on the module.
Starting MAC	Displays the starting MAC address for this module.

The **Stack Modules** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.

- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Displaying stack neighbors

To display information of the stack member neighbors, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Neighbors**.

The **Stack Neighbors** window is displayed as shown in Figure 20.

FIGURE 20 Monitoring stack neighbors

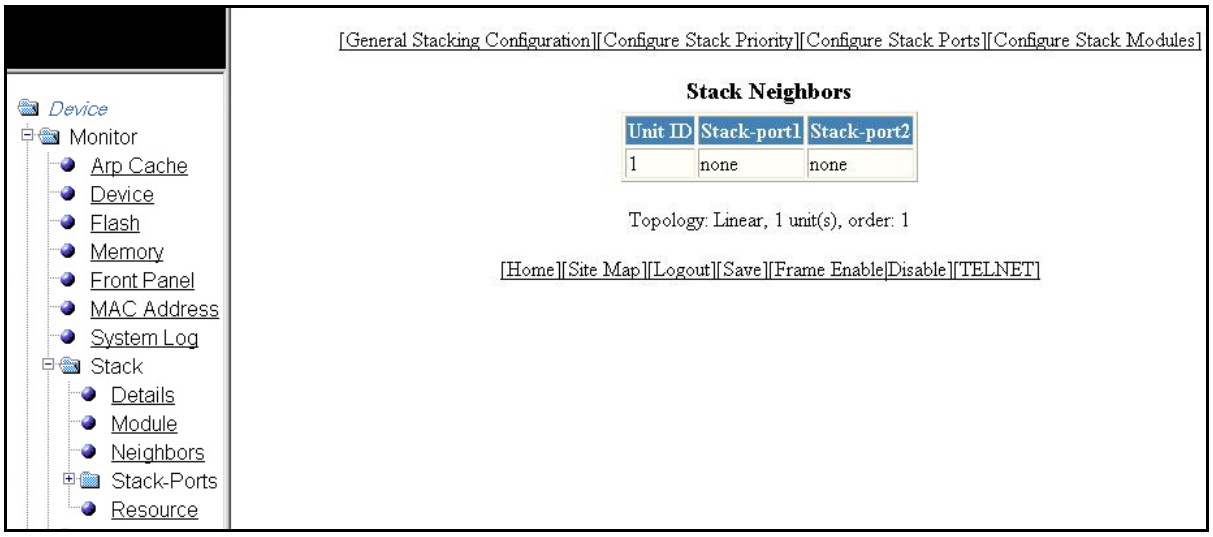


Table 9 describes the fields in the **Stack Neighbors** window.

TABLE 9 Description of the fields in the Stack Neighbors window

Field	Description
Unit ID	Displays the number of the unit within the stack from 1 through 8.
Stack-port1	Displays the neighbor stack unit for stack-port1 for this unit ID.
Stack-port2	Displays the neighbor stack unit for stack-port2 for this unit ID.
Topology	Displays either **Linear** or **Ring** stack topology of the connected devices.
unit(s)	Displays the number of units within the stack.
order	Displays the order of the unit IDs within the stack.

The **Stack Neighbors** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Displaying stack ports information

To display the information of the stack ports, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Stack-Ports** and then select **Status**.

The **Stack Port Status** window is displayed as shown in Figure 21.

FIGURE 21 Monitoring stack port status

Table 10 describes the fields in the **Stack Port Status** window.

TABLE 10 Description of the fields in the Stack Port Status window

Field	Description
Unit ID	Displays the number of the unit within the stack from 1 through 8.
Stack-port1	Displays the port state and the port number. The port states are as follows: • **up** – Each end is connected. • **down** – Port is configured as a stacking port, but not connected. • **none** – Port is not configured as a stacking port.

TABLE 10 Description of the fields in the **Stack Port Status** window (Continued)

Field	Description
Stack-port2	Displays the port state and the port number. The port states are: • **up** – Each end is connected. • **down** – Port is configured as a stacking port, but not connected. • **none** – Port is not configured as a stacking port.

The **Stack Port Status** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Displaying stack port statistics

To display stack port information for all ports in an IronStack topology, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Stack-Ports** and then select **Statistics**.

The **Stack Port Statistics** window is displayed as shown in Figure 22.

FIGURE 22 Monitoring stack port statistics

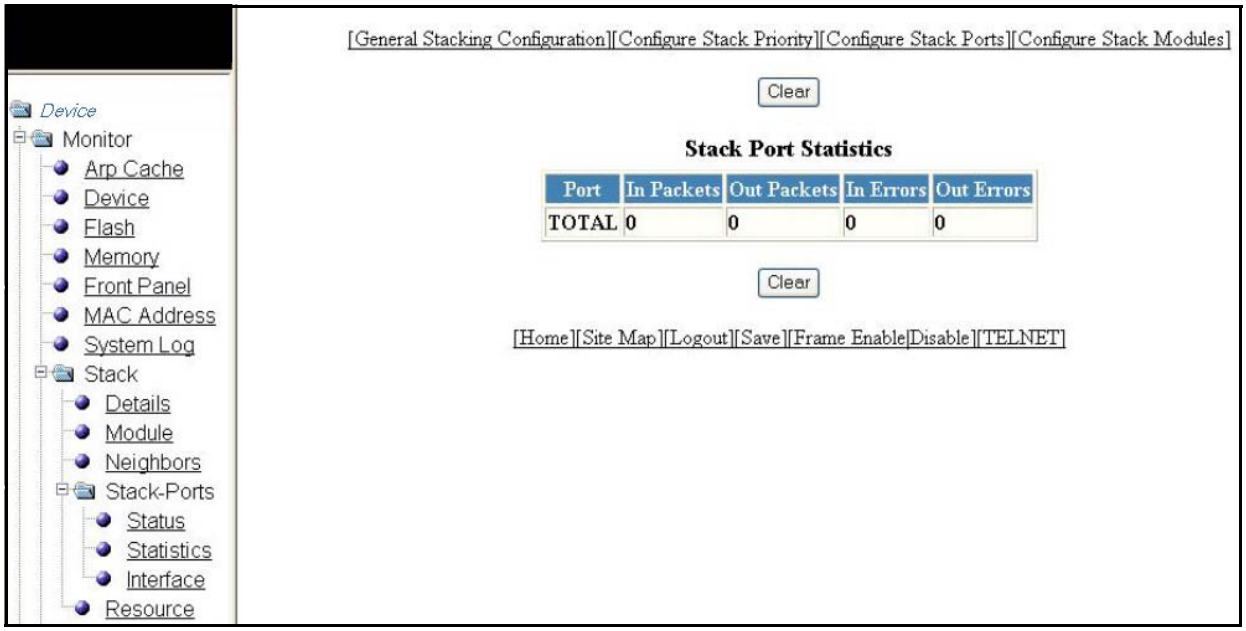


Table 11 describes the fields in the **Stack Port Statistics** window.

TABLE 11 Description of the fields in the **Stack Port Statistics** window

Field	Description
Port	Displays the stack identification number for this port.
In Packets	Displays the number of incoming packets on this port.
Out Packets	Displays the number of outgoing packets on this port.
In Errors	Displays the number of errors on the incoming packets on this port.
Out Errors	Displays the number of errors on the outgoing packets on this port.

To clear the information and begin a new monitoring cycle, click **Clear**. The **Stack Port Statistics** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Displaying stack port interfaces

To display information about stack port interfaces, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Stack-Ports** and then select **Interface**.

The **Stack Port Interface** window is displayed as shown in Figure 23.

FIGURE 23 Monitoring stack port interfaces

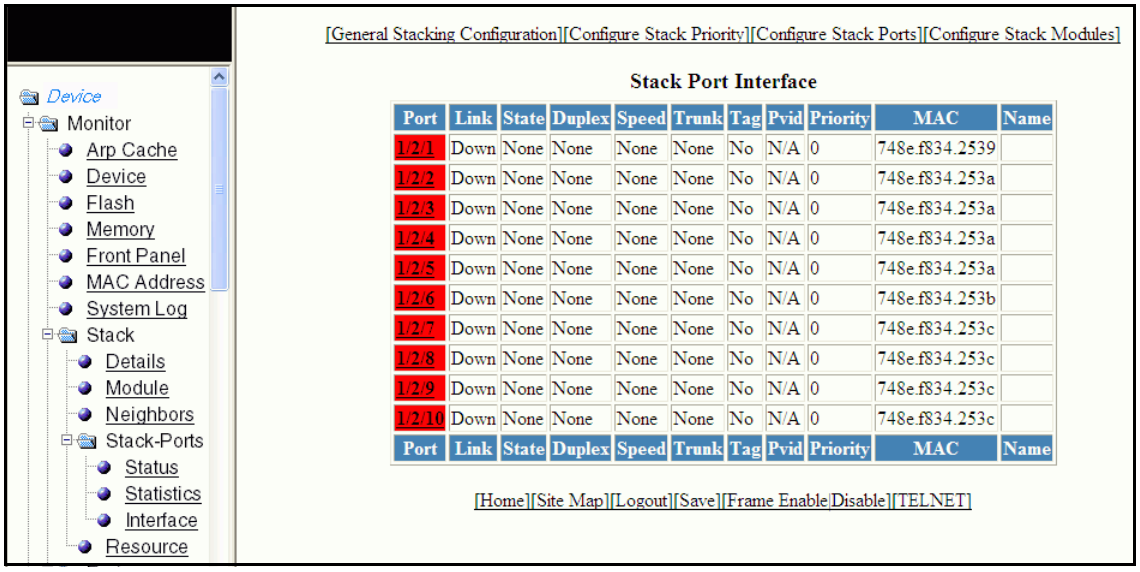

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Address
System Log
Stack
Details
Module
Neighbors
Stack-Ports
Status
Statistics
Interface
Resource
[General Stacking Configuration][Configure Stack Priority][Configure Stack Ports][Configure Stack Modules]
Stack Port Interface
Port Link State Duplex Speed Trunk Tag Pvid Priority MAC Name
1/2/1 Down None None None None No N/A 0 748e.f834.2539
1/2/2 Down None None None None No N/A 0 748e.f834.253a
1/2/3 Down None None None None No N/A 0 748e.f834.253a
1/2/4 Down None None None None No N/A 0 748e.f834.253a
1/2/5 Down None None None None No N/A 0 748e.f834.253a
1/2/6 Down None None None None No N/A 0 748e.f834.253b
1/2/7 Down None None None None No N/A 0 748e.f834.253c
1/2/8 Down None None None None No N/A 0 748e.f834.253c
1/2/9 Down None None None None No N/A 0 748e.f834.253c
1/2/10 Down None None None None No N/A 0 748e.f834.253c
Port Link State Duplex Speed Trunk Tag Pvid Priority MAC Name
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 12 describes the fields in the **Stack Port Interface** window.

TABLE 12 Description of the fields in the **Stack Port Interface** window

Field	Description
Port	Displays the stack identification number for this port.
Link	Displays whether the link is up or down.
State	Displays the state of the stack unit.
Duplex	Displays whether the port is configured as half or full duplex.
Speed	Displays the port speed as 10 Mbps, 100 Mbps, or 1000 Mbps.
Trunk	Displays the trunk group number, if the port is a member of a trunk group.
Tag	Displays whether the port is tagged or untagged.
Priority	Displays the port priority.
MAC	Displays the MAC address of the port.
Name	Displays the name assigned to the port.

The **Stack Port Interface** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Displaying stack resources

To display information about stack resources, perform the following steps.

1. Click **Monitor** on the left pane and select **Stack**.
2. Click **Resource**.

The **Stack Resource** window is displayed as shown in Figure 24.

FIGURE 24 Monitoring stack resources

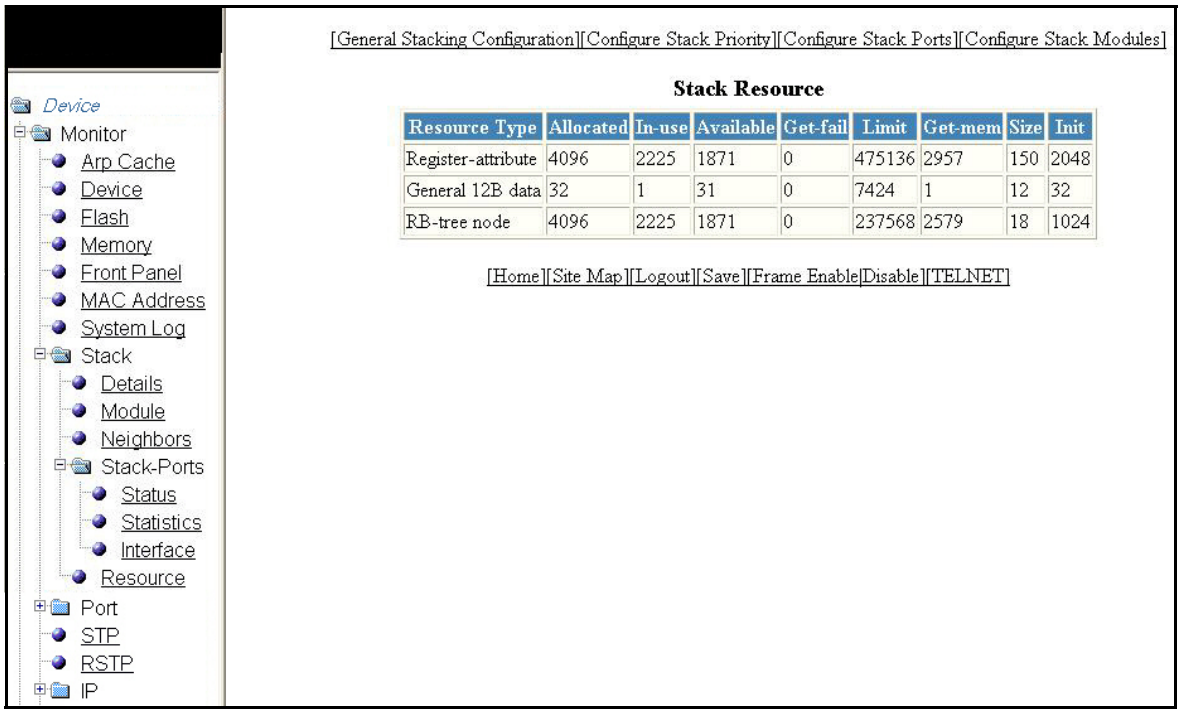


Table 13 describes the fields in the **Stack Resource** window.

TABLE 13 Description of the fields in the **Stack Resource** window

Field	Description
Resource Type	Displays the resource type as **Register-attributes**, **General 12B data**, or **RB-tree node**.
Allocated	Displays the amount of memory allocated for the stack.
In-use	Displays the amount of memory used by the stack.
Available	Displays the amount of free memory available.
Get-fail	Displays the number of get requests that have failed.
Limit	Displays the maximum amount of memory the system could allocate for a stack.
Get-mem	Displays the number of get-memory requests.
Size	Displays the size (bytes) for each stack resource.
Init	Displays the number of requests initiated.

The **Stack Resource** window provides links to configure the stack components:

- To change the stack settings, click **General Stacking Configuration**. For more information, refer to "Configuring the general settings for an IronStack" on page 125.
- To configure the priority of units within a stack, click **Configure Stack Priority**. For more information, refer to "Modifying stack priority" on page 126.
- To configure a stack port, click **Configure Stack Ports**. For more information, refer to "Modifying stack ports" on page 128.
- To configure a stack module, click **Configure Stack Modules**. For more information, refer to "Configuring a stack module" on page 129.

Chapter

4

Monitoring Ports

In this chapter

- Displaying Ethernet port statistics 35
- Displaying Ethernet port attributes 37
- Displaying Ethernet port utilization 39
- Displaying the management port information. 41
- Displaying port inline power for Brocade FCX and Brocade ICX 6610 devices 44
- Displaying port inline power for Brocade FSX devices 49

Displaying Ethernet port statistics

The **Ethernet Port Statistic** window lists the total number of packets, number of collisions, and number of errors that have occurred on a port. To display the Ethernet port statistics, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Statistic** and then select **Ethernet**.

   The **Ethernet Port Statistic** window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 25.
3. For Brocade FCX and Brocade ICX 6610 devices, select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available on the **Ethernet Port Statistic** window for Brocade FSX devices.

FIGURE 25 Monitoring Ethernet port statistics

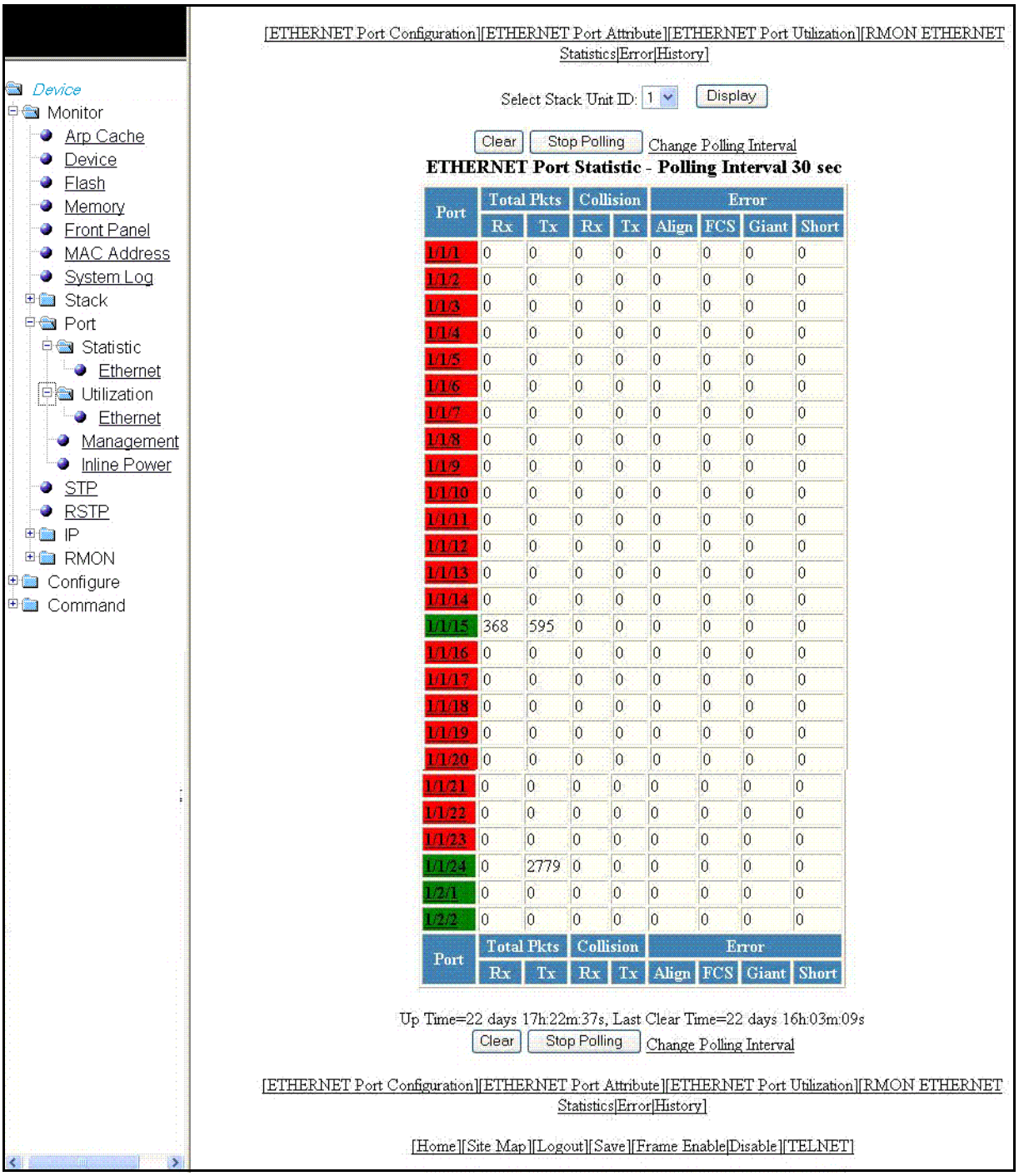

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Address
System Log
Stack
Port
Statistic
Ethernet
Utilization
Ethernet
Management
Inline Power
STP
RSTP
IP
RMON
Configure
Command
[ETHERNET Port Configuration][ETHERNET Port Attribute][ETHERNET Port Utilization][RMON ETHERNET Statistics|Error|History]
Select Stack Unit ID: 1
Display
Clear
Stop Polling
Change Polling Interval
ETHERNET Port Statistic - Polling Interval 30 sec
Port
Total Pkts
Collision
Error
Rx
Tx
Rx
Tx
Align
FCS
Giant
Short
1/1/1 0 0 0 0 0 0 0 0
1/1/2 0 0 0 0 0 0 0 0
1/1/3 0 0 0 0 0 0 0 0
1/1/4 0 0 0 0 0 0 0 0
1/1/5 0 0 0 0 0 0 0 0
1/1/6 0 0 0 0 0 0 0 0
1/1/7 0 0 0 0 0 0 0 0
1/1/8 0 0 0 0 0 0 0 0
1/1/9 0 0 0 0 0 0 0 0
1/1/10 0 0 0 0 0 0 0 0
1/1/11 0 0 0 0 0 0 0 0
1/1/12 0 0 0 0 0 0 0 0
1/1/13 0 0 0 0 0 0 0 0
1/1/14 0 0 0 0 0 0 0 0
1/1/15 368 595 0 0 0 0 0 0
1/1/16 0 0 0 0 0 0 0 0
1/1/17 0 0 0 0 0 0 0 0
1/1/18 0 0 0 0 0 0 0 0
1/1/19 0 0 0 0 0 0 0 0
1/1/20 0 0 0 0 0 0 0 0
1/1/21 0 0 0 0 0 0 0 0
1/1/22 0 0 0 0 0 0 0 0
1/1/23 0 0 0 0 0 0 0 0
1/1/24 0 2779 0 0 0 0 0 0
1/2/1 0 0 0 0 0 0 0 0
1/2/2 0 0 0 0 0 0 0 0
Port
Total Pkts
Collision
Error
Rx
Tx
Rx
Tx
Align
FCS
Giant
Short
Up Time=22 days 17h:22m:37s, Last Clear Time=22 days 16h:03m:09s
Clear
Stop Polling
Change Polling Interval
[ETHERNET Port Configuration][ETHERNET Port Attribute][ETHERNET Port Utilization][RMON ETHERNET Statistics|Error|History]
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 14 describes the fields in the **ETHERNET Port Statistic** window.

TABLE 14 Description of the fields in the **ETHERNET Port Statistic** window

Field	Description
Port	Displays the port number for which the statistics were collected.
Total Packets	Displays the total number of packets received (**Rx**) and transmitted (**Tx**) on the port.
Collision	Shows the number of received (**Rx**) and transmitted (**Tx**) collisions on the port.
Error	Displays the number of errors on the port for the following types: • **Alignment** – Packets with frame alignment errors. • **FCS** – Packets with frame check sequence errors. • **Giant** – Packets that were longer than the configured MTU. • **Short** – Packets that were shorter than the minimum valid length.

To remove the current data and restart the monitoring process, click **Clear**. To stop the polling process, click **Stop Polling.** You can also change the current polling interval by clicking **Change Polling Interval**.

The **ETHERNET Port Statistic** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to "Configuring an Ethernet port" on page 175.
- To monitor the Ethernet port attributes, click **ETHERNET Port Attribute**. For more information, refer to "Displaying Ethernet port attributes" on page 37.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to "Displaying Ethernet port utilization" on page 39.
- To monitor Remote Monitoring (RMON) statistics, click **RMON ETHERNET Statistics Error**. For more information, refer to "Displaying RMON Ethernet statistics" on page 117.
- To monitor RMON history, click **RMON ETHERNET Statistics History**. For more information, refer to "Displaying RMON history" on page 115.

Displaying Ethernet port attributes

The **Port Attributes** window lists the number, state, media, connector, and MAC address of the port. To display the Ethernet port attribute information, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Statistic** and then select **Ethernet**.
3. Click **ETHERNET Port Attribute** on the **ETHERNET Port Statistic** window.
4. For Brocade FCX and Brocade ICX 6610 devices, select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available on the **Port Attributes** window for Brocade FSX devices.

The **Port Attributes** window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 26.

FIGURE 26 Monitoring Ethernet port attributes

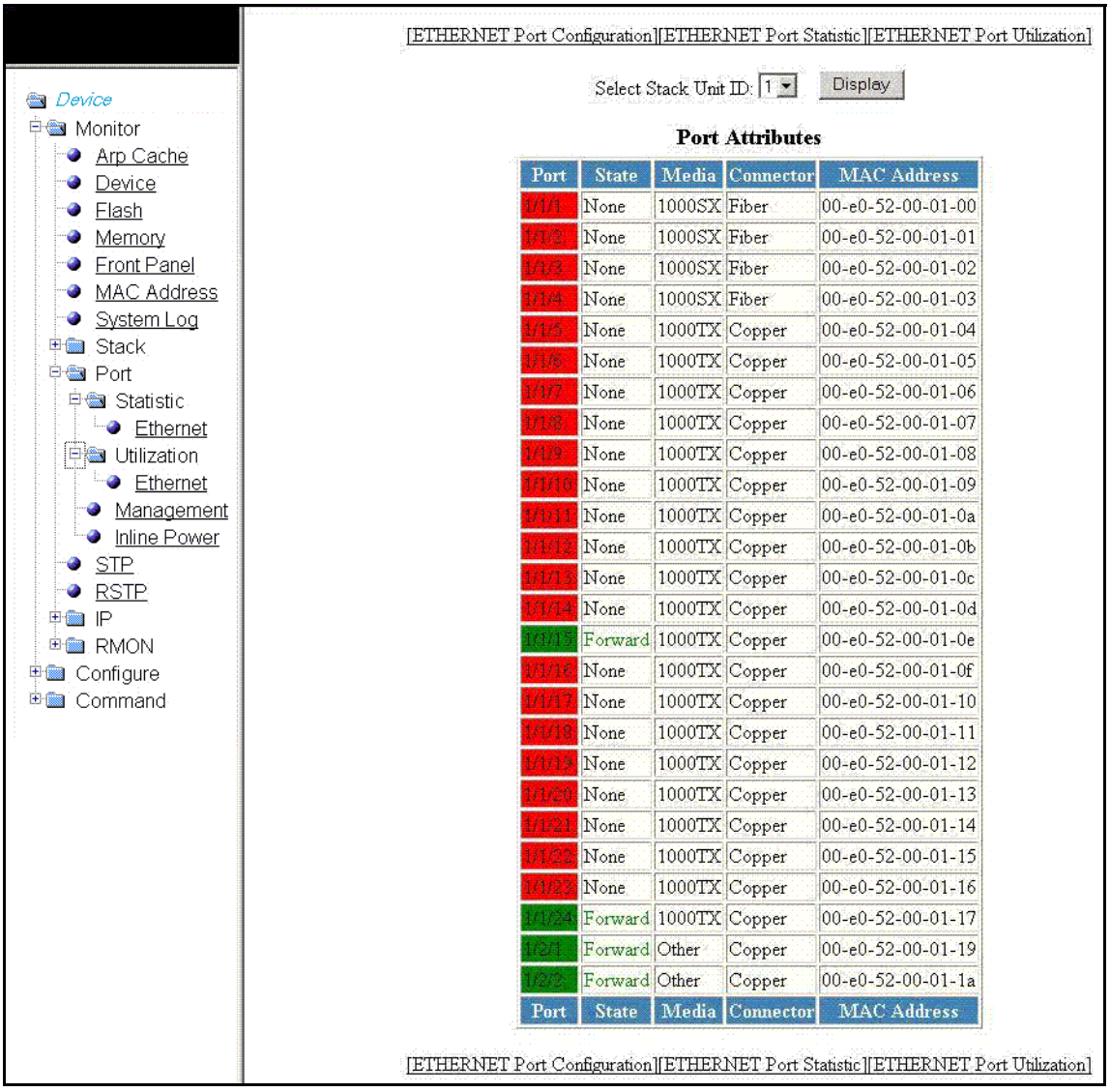


Table 15 describes the fields in the **Port Attributes** window.

TABLE 15 Description of the fields in the **Port Attributes** window

Field	Description
Port	Displays the port number.
State	Displays the status of the port.
Media	Displays the type of the Ethernet cable used.
Connector	Displays the physical type of connector.
MAC Address	Displays the Media Access Control (MAC) address of the port.

The **Port Attributes** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to "Configuring an Ethernet port" on page 175.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to "Displaying Ethernet port statistics" on page 35.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to "Displaying Ethernet port utilization" on page 39.

Displaying Ethernet port utilization

The **Ethernet Port Utilization** window lists the traffic that is received and transmitted on a port. To display the Ethernet port utilization information, perform the following steps.

1. Click **Monitor** on the left pane and select **Port.**
2. Click **Utilization** and then select **Ethernet**.

   The **Ethernet Port Utilization** window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 27.
3. For Brocade FCX and Brocade ICX 6610 devices, select a unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available on the **ETHERNET Port Utilization** window for Brocade FSX devices.

FIGURE 27 Monitoring Ethernet port utilization

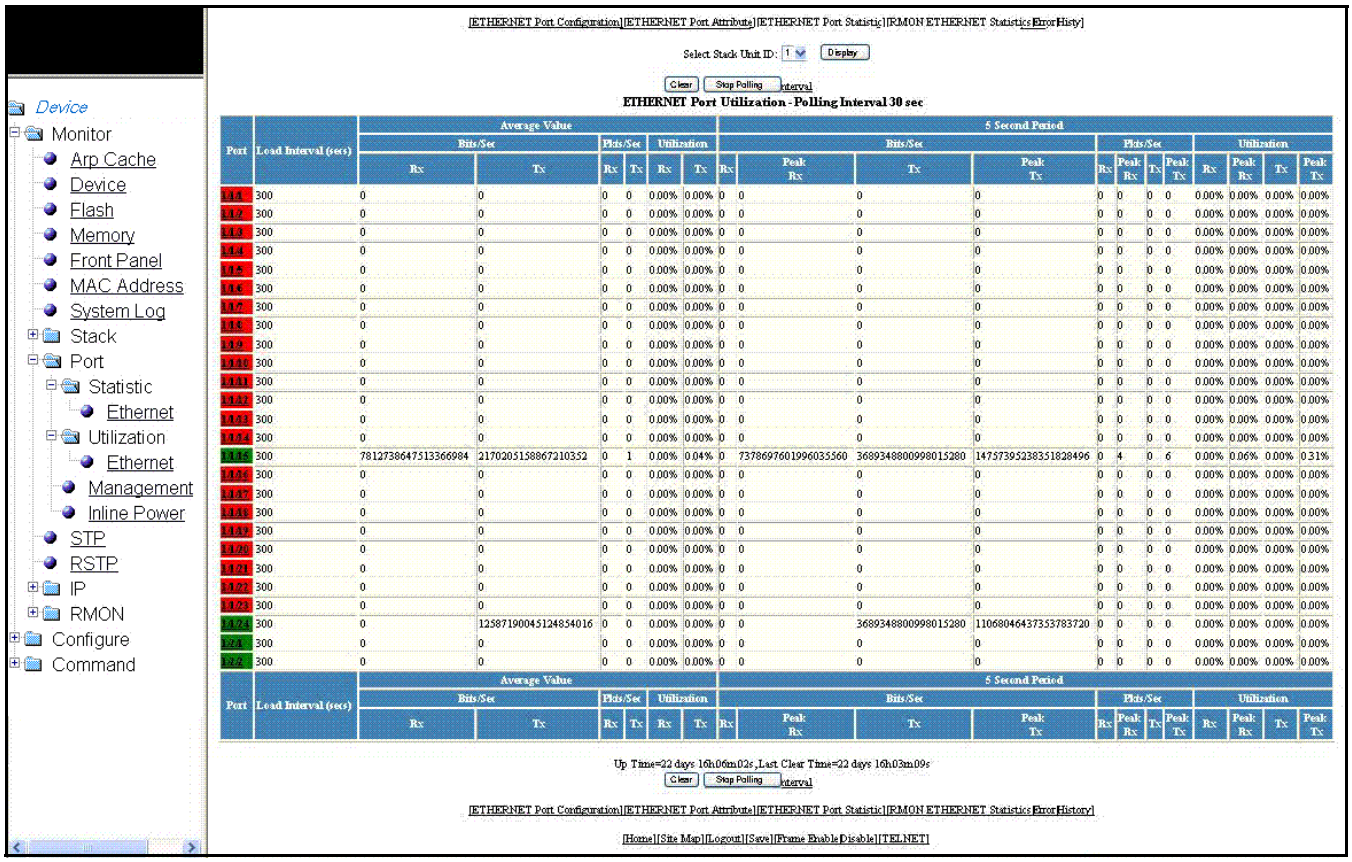


Table 16 describes the fields in the **ETHERNET Port Utilization** window.

TABLE 16 Description of the fields in the **ETHERNET Port Utilization** window

Field	Description
Port	Displays the port number. Each entry has a link to detailed information about the port.
Load Interval (secs)	Displays the number of seconds for which average port utilization should be calculated. This object can have a value from 30 through 300, in 30-second increments. The default value is 300 seconds.
Average Value	Displays the following information: • **Bits/Sec** – The average number of bits per second received and transmitted on the port. • **Pkts/Sec** – The average number of packets per second received and transmitted on the port. • **Utilization** – The average percent utilization received and transmitted on the port.
5 Second Period	This set of columns show the number of bits per second (**Bits/Sec**), number of packets per second (**Pkts/Sec**), and utilization percentages (**Utilization**) received and transmitted on a port at each 5 second interval. Peak activities for each category are also provided.

To remove the current data and restart the monitoring process, click **Clear**. To stop the statistics polling process, click **Stop Polling.** You can also change the current polling interval by clicking **Change Polling Interval**.

The **ETHERNET Port Utilization** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to "Configuring an Ethernet port" on page 175.
- To monitor the Ethernet port attributes, click **ETHERNET Port Attribute**. For more information, refer to "Displaying Ethernet port attributes" on page 37.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to "Displaying Ethernet port statistics" on page 35.
- To monitor Remote Monitoring (RMON) statistics, click **RMON ETHERNET Statistics Error**. For more information, refer to "Displaying RMON Ethernet statistics" on page 117.
- To monitor RMON history, click **RMON ETHERNET Statistics History**. For more information, refer to "Displaying RMON history" on page 115.

Displaying the management port information

To display the current management port configuration information, perform the following steps.

1. Click **Monitor** on the left pane and select **Port.**
2. Click **Management**.

The **Management Port Configuration** window is displayed as shown in Figure 28.

FIGURE 28 Monitoring a management port configuration

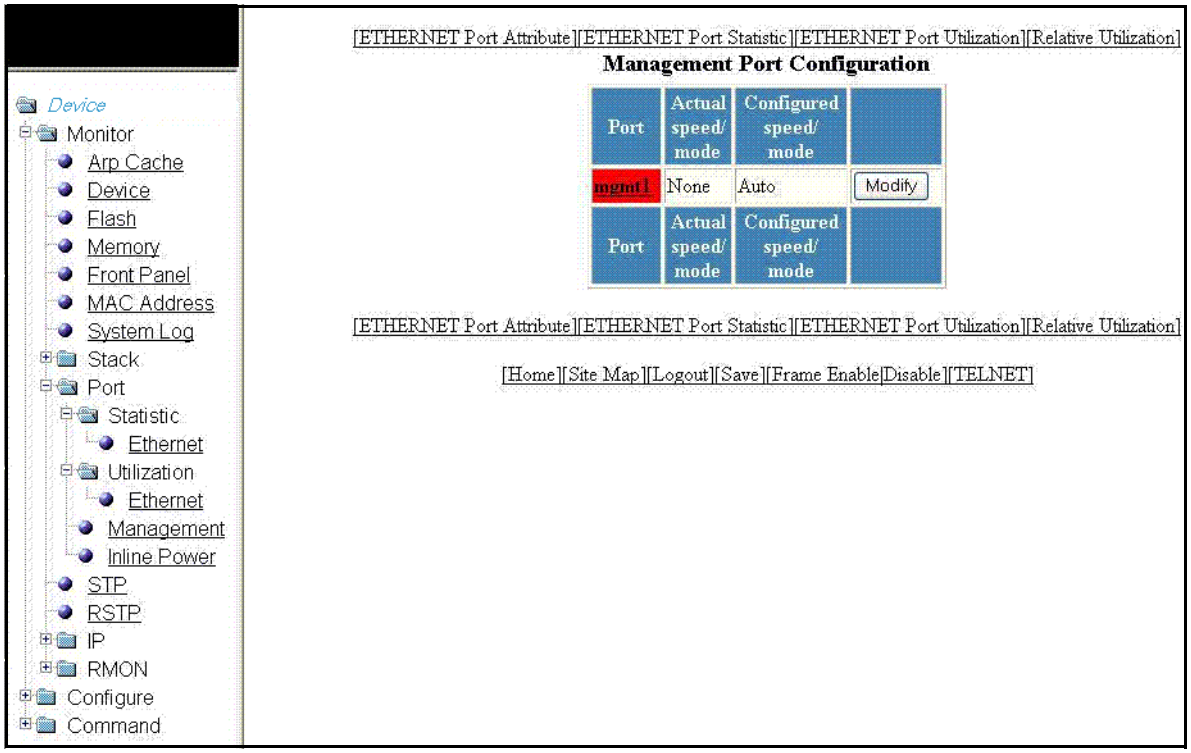


Table 17 describes the fields in the **Management Port Configuration** window.

TABLE 17 Description of the fields in the **Management Port Configuration** window

Field	Description
Port	Displays the name of the management port. Each entry has a link to detailed real-time information about the port. Refer to "Displaying the management port real-time information".
Actual speed/mode	Shows whether the actual speed matches the configured speed. If the configured speed is set to **Auto**, then the speed is set by the software.
Configured speed/mode	The speed duplex set for the port.

To configure a management port or change the configuration of a current management port, click **Modify**. For more information, refer to "Configuring a management port" on page 178.

The **Management Port Configuration** window provides links to configure the port parameters:

- To monitor the Ethernet port attributes, click **ETHERNET Port Attribute**. For more information, refer to "Displaying Ethernet port attributes" on page 37.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to "Displaying Ethernet port statistics" on page 35.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to "Displaying Ethernet port utilization" on page 39.
- To configure the port uplink utilization list, click **Relative Utilization**. For more information, refer to "Configuring the port uplink relative utilization" on page 179.

Displaying the management port real-time information

To display the real-time information of a port, click on the management port (for example, **mgmt1**).

The **Port Realtime Information** window is displayed as shown in Figure 29.

FIGURE 29 Monitoring management port real-time information

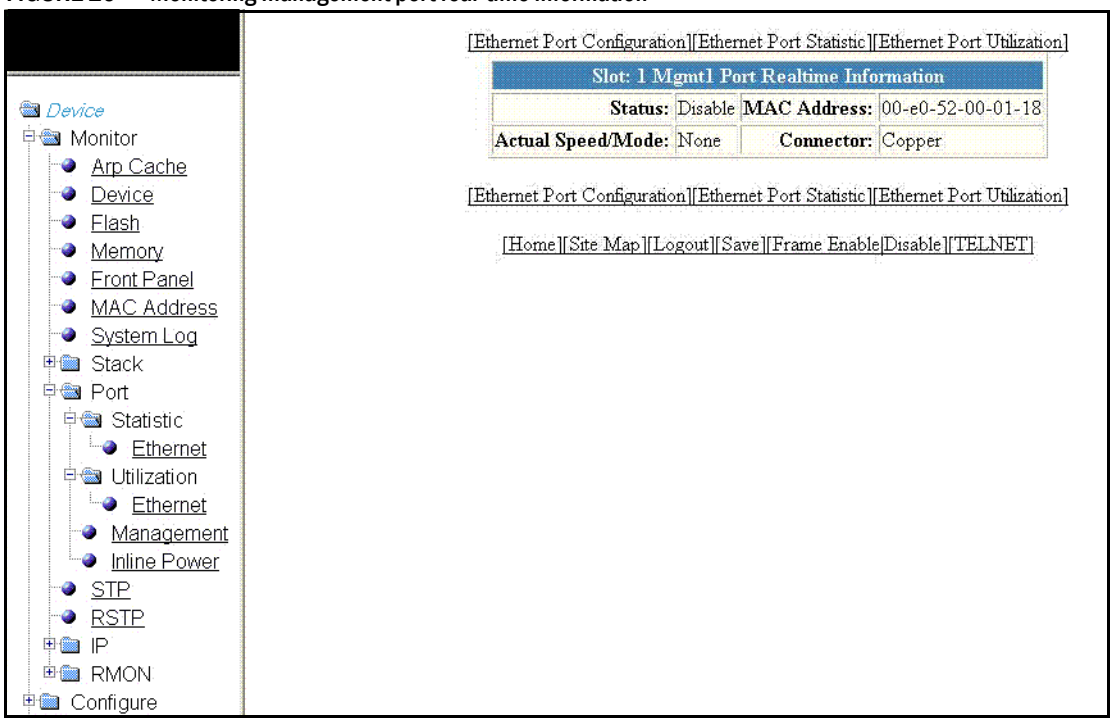


Table 18 describes the fields in the **Port Realtime Information** window.

TABLE 18 Description of the fields in the **Port Realtime Information** window

Field	Description
Status	Displays the status of the port.
MAC Address	Displays the MAC address of the port.
Actual Speed/Mode	Shows whether the actual speed matches the configured speed. If the configured speed is set to Auto, then the speed is set by the software.
Connector	Displays the physical type of connector.

The **Port Realtime Information** window provides links to configure the port parameters:

- To configure an Ethernet port, click **ETHERNET Port Configuration**. For more information on how to configure an Ethernet port, refer to "Configuring an Ethernet port" on page 175.
- To monitor the Ethernet port statistics, click **ETHERNET Port Statistic**. For more information, refer to "Displaying Ethernet port statistics" on page 35.
- To monitor the Ethernet port utilization, click **ETHERNET Port Utilization**. For more information, refer to "Displaying Ethernet port utilization" on page 39.

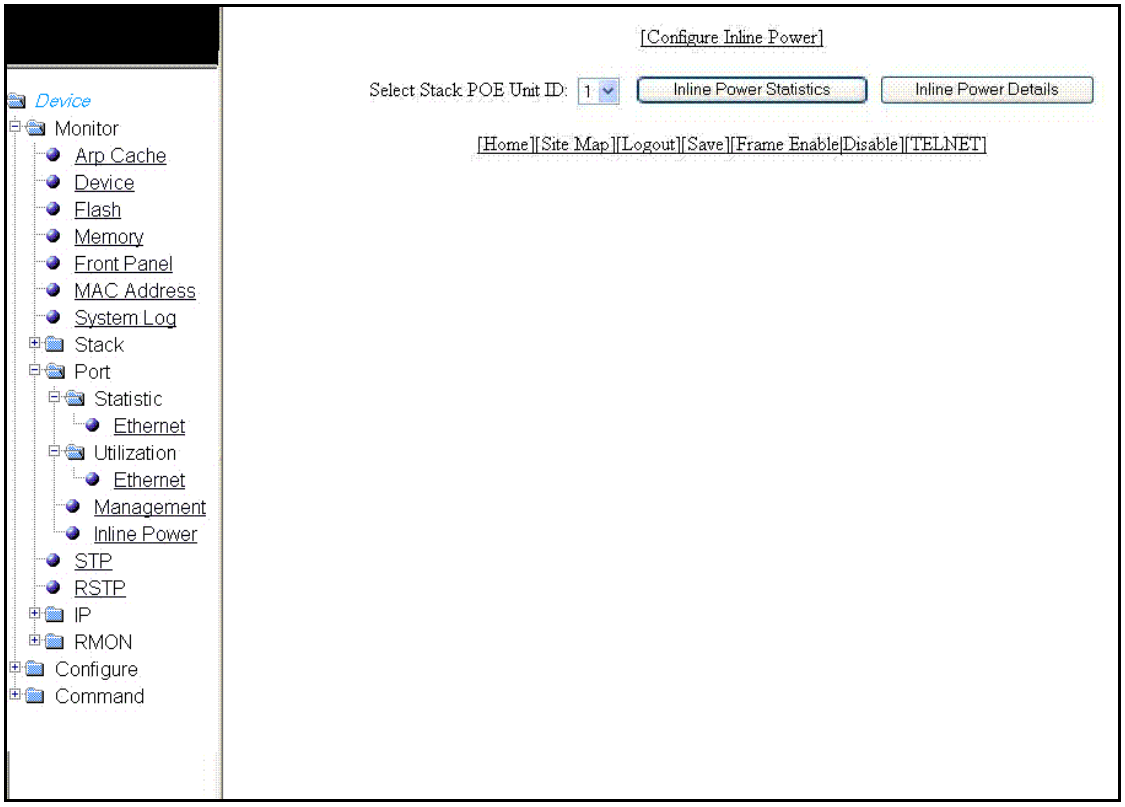
Displaying port inline power for Brocade FCX and Brocade ICX 6610 devices

The port inline power statistics allow you to monitor Power over Ethernet (PoE), the ability to transfer electrical power and data to remote devices over standard twisted-pair cable in an Ethernet network. To display the inline power statistics for a PoE stack device, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Inline Power**.

   The port inline power window is displayed as shown in Figure 30.
3. Select a unit ID in the **Select Stack POE Unit ID** list and click either **Inline Power Statistics** or **Inline Power Details**.

FIGURE 30 Monitoring inline power



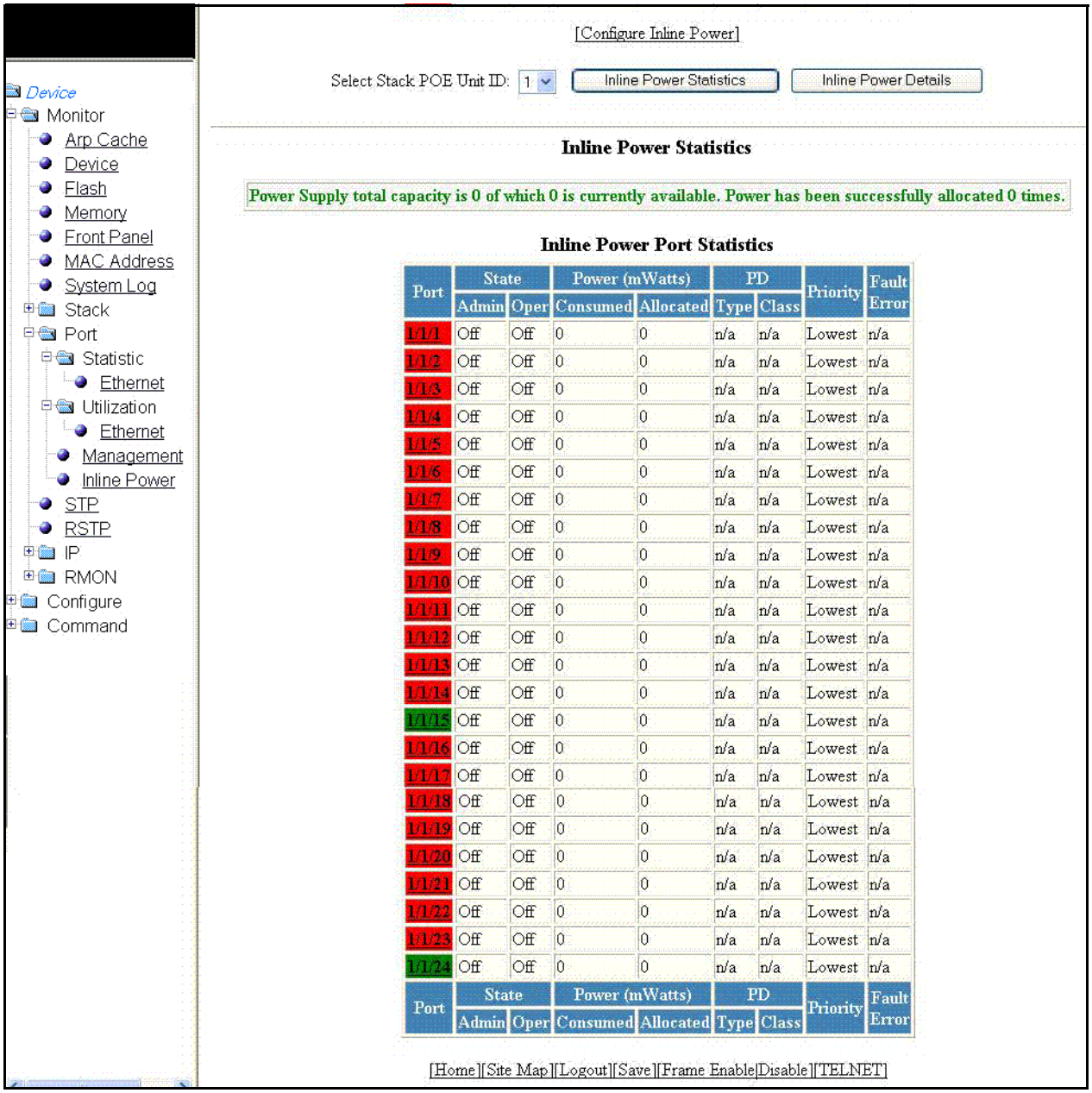
NOTE
Only PoE-capable units are displayed in the **Select Stack POE Unit ID** list. If there are no PoE units, you will receive **No units with POE modules** as an error message.

Displaying inline power statistics

To display the inline power statistics, select the unit ID in the **Select Stack POE Unit ID** list and click **Inline Power Statistics**.

The **Inline Power Statistics** window is displayed as shown in Figure 31.

FIGURE 31 Monitoring inline power statistics



Port	State		Power (mWatts)		PD		Priority	Fault Error
	Admin	Oper	Consumed	Allocated	Type	Class		
1/1/1	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/2	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/3	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/4	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/5	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/6	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/7	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/8	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/9	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/10	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/11	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/12	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/13	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/14	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/15	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/16	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/17	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/18	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/19	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/20	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/21	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/22	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/23	Off	Off	0	0	n/a	n/a	Lowest	n/a
1/1/24	Off	Off	0	0	n/a	n/a	Lowest	n/a
Port	State		Power (mWatts)		PD		Priority	Fault Error
	Admin	Oper	Consumed	Allocated	Type	Class		

Table 19 describes the fields in the **Inline Power Statistics** window.

TABLE 19 Description of the fields in the **Inline Power Statistics** window

Field	Description
Port	Displays the stack port identification of the port as stack#/slot#/port#.
State: Admin	Specifies whether PoE has been enabled on the port, using one of the following values: • **ON** – The inline power command was issued on the port. • **OFF** – The inline power command has not been issued on the port.
State: Oper	Displays the status of inline power on the port, using one of the following values: • **ON** – The PoE power supply is delivering inline power to the powered device. • **OFF** – The PoE power supply is not delivering inline power to the powered device. • **DENIED** – The port is in standby mode waiting for power because currently there is not enough available power for the port.
Power (mWatts) Consumed	Displays the amount of current (milliwatts) the powered device is consuming.
Power (mWatts) Allocated	Displays the amount of current (milliwatts) allocated to the port. This value is either the default or configured maximum power level, or the power class that was automatically detected.
PD Type	Displays the type of powered device connected to the port. This value can be one of the following: • **802.3at** - The PD connected to this port is 802.3at-compliant. • **802.3af** - The PD connected to this port is 802.3af-compliant. • **LEGACY** – The powered device connected to this port is a legacy product (not 802.3af-compliant). • **N/A** – One of the following is true: - The device connected to this port is a non-powered device. - No device is connected to this port. - The port is in standby or denied mode (waiting for power).
PD Class	Displays the maximum amount of power received by a powered device. This value can be one of the following: • **Class1** – Receives 4 watts maximum. • **Class2** – Receives 7 watts maximum. • **Class3** – Receives 15.4 watts maximum. • **Class 4** - Receives 30 watts maximum. • **n/a** – The device attached to the port cannot advertise its class.
Priority	Displays the inline power priority of the port, which determines the order in which the port receives power while in standby mode (waiting for power). Ports with a higher priority receive power before ports with a low priority. The value of priority can be one of the following: • **1** – Critical priority • **2** – High priority • **3** – Low priority

TABLE 19 Description of the fields in the **Inline Power Statistics** window (Continued)

Field	Description
Fault Error	Displays the fault or error that occurred on the port, if applicable. Otherwise, **n/a** is dispalyed. The value can be one of the following: • critical temperature – The PoE chip temperature limit rose above the safe operating level, thereby powering down the port. • detection failed - discharged capacitor – The port failed capacitor detection (legacy PD detection) because of a discharged capacitor. This can occur when connecting a non-PD on the port. • detection failed - out of range capacitor – The port failed capacitor detection (legacy PD detection) because of an out-of-range capacitor value. This can occur when connecting a non-PD on the port. • internal h/w fault – A hardware problem has hindered port operation. • lack of power – The port has shut down due to lack of power. • main supply voltage high – The voltage was higher than the maximum voltage limit, thereby tripping the port. • main supply voltage low – The voltage was lower than the minimum voltage limit, thereby tripping the port. • overload state – The PD consumes more power than the maximum limit configured on the port, based on the default configuration, user configuration, or CDP configuration. • over temperature – The port temperature rose above the temperature limit, thereby powering down the port. • PD DC fault – A succession of underload and overload states, or a PDDC/DC fault, caused the port to shutdown. • short circuit – A short circuit was detected on the port delivering power. • underload state – The PD consumes less power than the minimum limit specified in the 802.3af standard. • voltage applied from ext src – The port failed capacitor detection (legacy PD detection) because the voltage applied to the port was from an external source.

Displaying inline power details

To display the inline power details, select the unit ID in the **Select Stack POE Unit ID** list and click **Inline Power Details**.

The **Inline Power Details** window is displayed as shown in Figure 32.

FIGURE 32 Monitoring inline power details

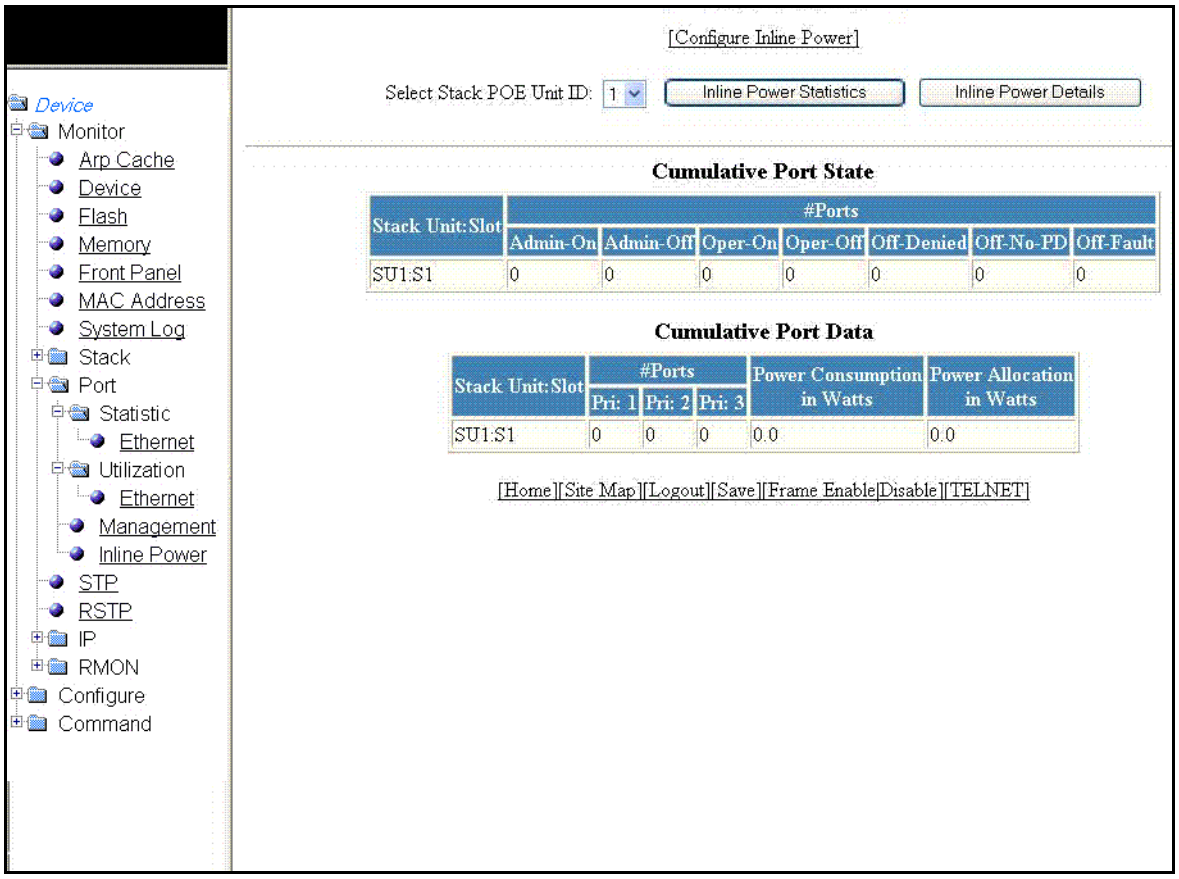


Table 20 describes the fields in the **Inline Power Details** window.

TABLE 20 Description of the fields in the **Inline Power Details** window

Field	Description
Cumulative Port State parameters	
Stack Unit: Slot	Displays the stack ID and slot ID from 1 through 2. The PoE-capable slots are available on PoE stack units.
# Ports Admin-On	Displays the number of ports on the interface module on which the inline power was configured.
# Ports Admin-Off	Displays the number of ports on the interface module on which the inline power was not configured.
# Port Oper-On	Displays the number of ports on the Interface module that are receiving inline power from the PoE power supply.
# Port Oper-Off	Displays the number of ports on the Interface module that are not receiving inline power from the PoE power supply.
# Ports Off-Denied	Displays the number of ports on the Interface module that were denied power because of insufficient power.
# Ports Off No-PD	Displays the number of ports on the Interface module to which no powered device (PDs) are connected.

TABLE 20 Description of the fields in the **Inline Power Details** window (Continued)

Field	Description
# Ports Off-Fault	Displays the number of ports on the Interface module that are not receiving power because of a subscription overload.
Cumulative Port Data parameters	
Stack Unit: Slot	Displays the stack ID and slot ID from 1 through 2. The PoE-capable slots are available on PoE stack units.
# Ports	Displays the total number of available ports in each level of priority.
Power Consumption in Watts	Displays the total number of watts consumed by both PoE power consuming devices and the PoE module (daughter card) attached to the Interface module.
Power Allocation in Watts	Displays the number of watts allocated to the interface module PoE ports. This value is the sum of port default or configured maximum power levels, or power classes automatically detected by the PoE device.

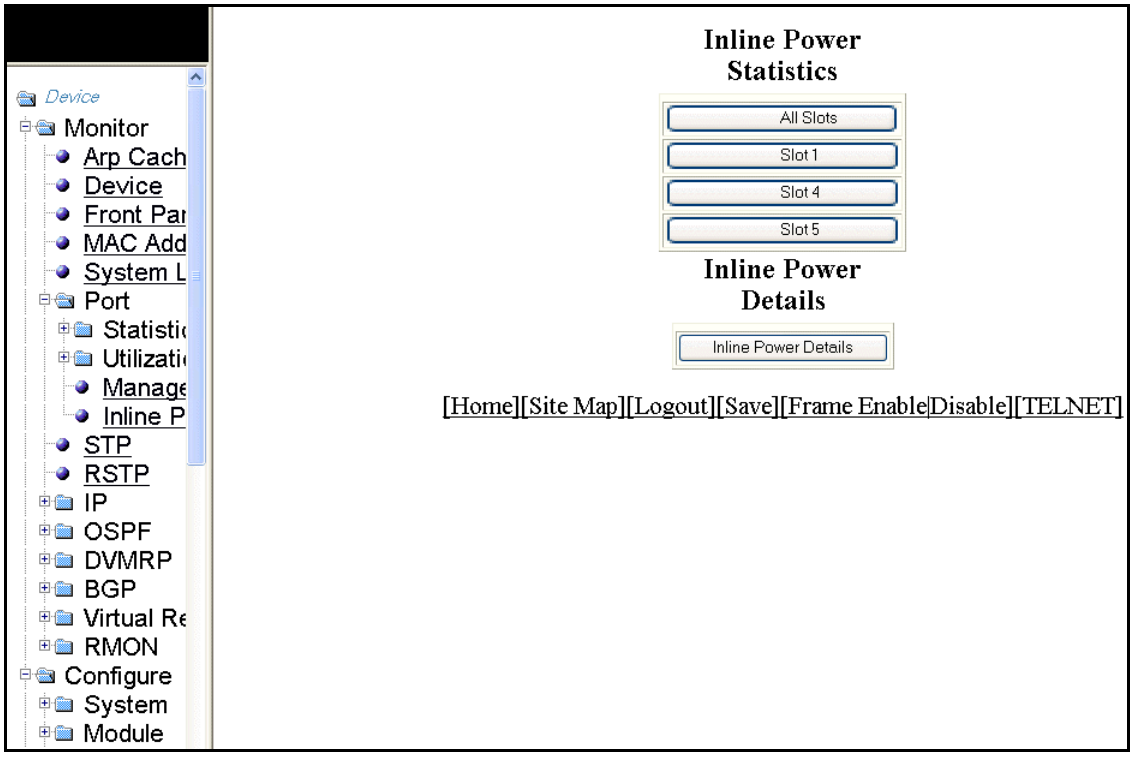
Displaying port inline power for Brocade FSX devices

To display the inline power statistics for a Brocade FSX device, perform the following steps.

1. Click **Monitor** on the left pane and select **Port**.
2. Click **Inline Power**.

The port inline power window is displayed as shown in Figure 33.

FIGURE 33 Monitoring inline power



3. Click **All Slots** to display the inline power statistics of all the slots.
4. Click **Slot 1**, **Slot 4**, or **Slot 5** to display the inline power statistics for the individual slot.
5. Click **Inline Power Details** to display detailed operational information about the PoE power supplies.

Chapter

Monitoring STP

5

In this chapter

- Displaying STP information 51

Displaying STP information

Brocade Layer 2 switches and Layer 3 switches support standard Spanning Tree Protocol (STP) as described in the IEEE 802.1D specification. By default, STP is enabled on Layer 2 switches and disabled on Layer 3 switches. To display the STP information, perform the following steps.

1. Click **Monitor** on the left pane and select **STP**.

   By default, STP is disabled on Layer 3 switches and therefore the message **STP is disabled. Go to system to enable STP** is displayed.

2. For Brocade FCX and Brocade ICX 6610 devices, select a stack unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available in the STP window for Brocade FSX devices.

The STP window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 34.

FIGURE 34 Monitoring the STP bridge and port

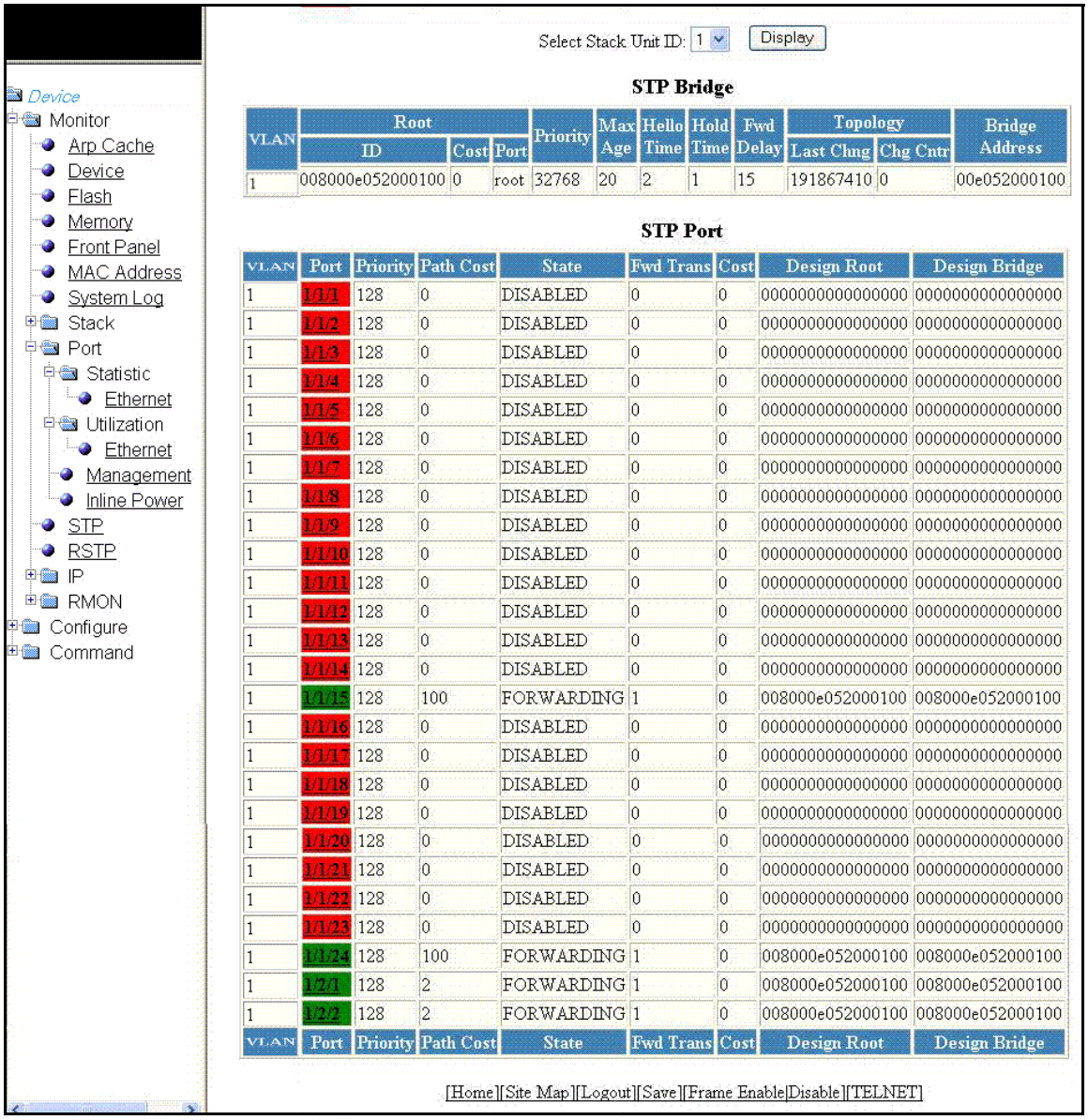


Table 21 describes the fields in the STP window.

TABLE 21 Description of the fields in the STP window

Field	Description
STP Bridge parameters (global parameters)	
VLAN	Displays the port-based virtual local area network (VLAN) that contains this spanning tree (instance of STP). VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all STP information is for VLAN 1.
Root ID	Displays the ID assigned by STP to the root bridge for this spanning tree.
Root Cost	Displays the cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.

TABLE 21 Description of the fields in the STP window (Continued)

Field	Description
Root Port	Displays the port on this device that connects to the root bridge. If this device is the root bridge, then the value is **root** instead of a port number.
Priority	Displays the STP priority of this device or VLAN. The value is shown in hexadecimal format.
Max Age	Displays the number of seconds this device or VLAN waits for a Hello message from the root bridge before deciding that the root has become unavailable and performing a reconvergence.
Hello Time	Displays the interval between each configuration Bridge Packet Data Unit (BPDU) sent by the root bridge.
Hold Time	Displays the minimum number of seconds that must elapse between transmissions of consecutive configuration BPDUs on a port.
Fwd Delay	Displays the number of seconds this device or VLAN waits following a topology change and consequent reconvergence.
Topology Last Chng	Displays the number of seconds since the last time a topology change occurred.
Topology Chg Cntr	Displays the number of times the topology has changed since the device was reloaded.
Bridge Address	Displays the STP address of this device or VLAN.
STP Port parameters	
VLAN	Displays the VLAN that the port is in. This field displays only when port VLAN is enabled.
Port	Displays the port number. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Priority	Displays the STP priority of the port in hexadecimal format.
Path Cost	Displays the STP path cost of the port.
State	Displays the STP state of the port. The state can be one of the following: • **BLOCKING** – STP has blocked Layer 2 traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in the BLOCKING state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. • **DISABLED** – The port is not participating in STP. This can occur when the port is disconnected or STP is disabled on the port. • **FORWARDING** – STP is allowing the port to send and receive frames. • **LISTENING** – STP is responding to a topology change and this port is listening for a BPDU from neighboring bridges in order to determine the new topology. No frames are transmitted or received during this state. • **LEARNING** – The port has passed through the LISTENING state and will change to the BLOCKING or FORWARDING state depending on the results of STP's reconvergence. The port does not transmit or receive frames during this state. However, the device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.
Fwd Trans	Displays the number of times STP has changed the state of this port between BLOCKING and FORWARDING.
Cost	Displays the cost to the root bridge as advertised by the designated bridge that is connected to this port. If the designated bridge is the root bridge itself, then the cost is 0.

TABLE 21 Description of the fields in the STP window (Continued)

Field	Description
Design Root	Displays the root bridge as recognized on this port. The value is the same as the root bridge ID listed in the **Root ID** field.
Design Bridge	Displays the designated bridge to which this port is connected. The designated bridge is the device that connects the network segment on the port to the root bridge.

Chapter

Monitoring RSTP

6

In this chapter

- Displaying RSTP information 55

Displaying RSTP information

To view current Rapid Spanning Tree Protocol (RSTP) information for a device, you must configure RSTP. For more information on how to configure RSTP, refer to Chapter 22, "Configuring RSTP". By default, RSTP is enabled on Layer 2 switches and disabled on Layer 3 switches.

To display RSTP bridge and port information, click **Monitor** on the left pane and select **RSTP**.

The RSTP window is displayed as shown in Figure 35.

FIGURE 35 Monitoring the RSTP bridge and port

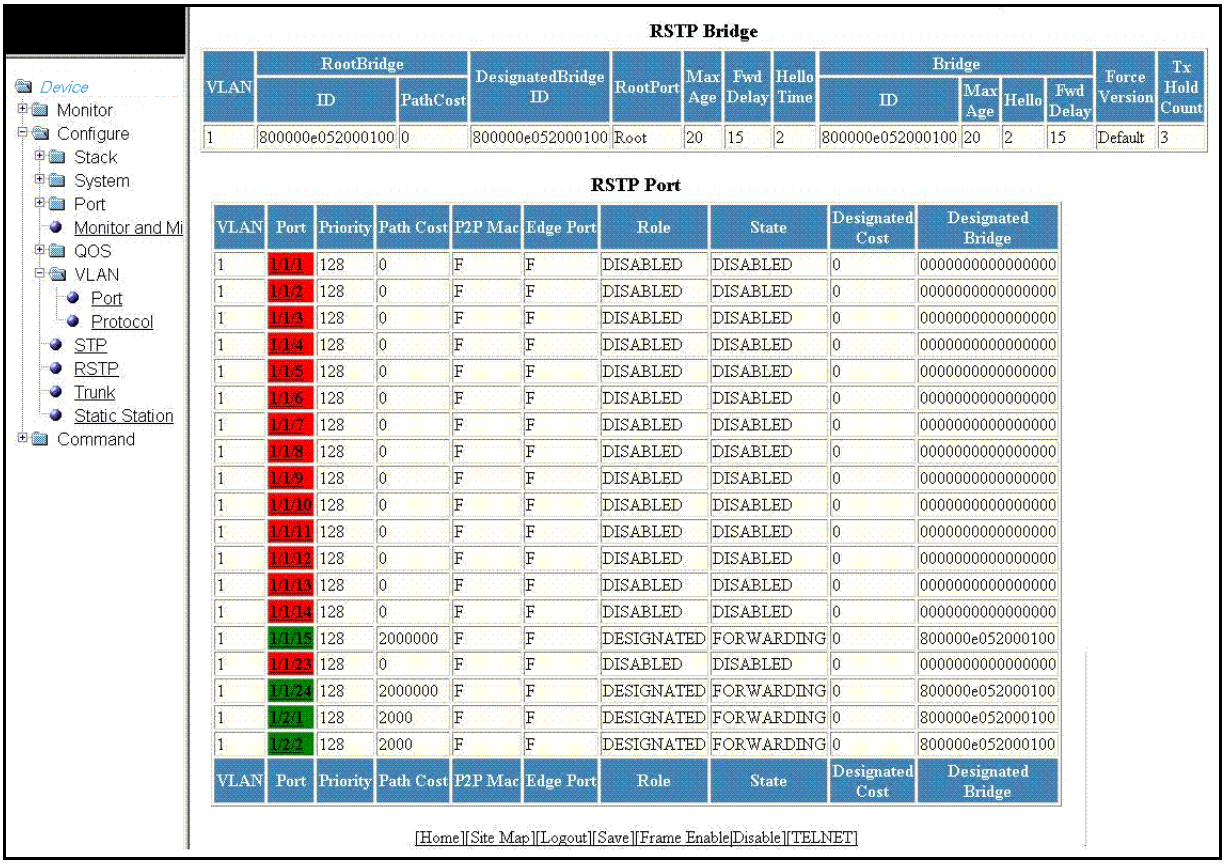

Device
Monitor
Configure
Stack
System
Port
Monitor and Mi
QOS
VLAN
Port
Protocol
STP
RSTP
Trunk
Static Station
Command
RSTP Bridge
VLAN
RootBridge
ID
PathCost
DesignatedBridge ID
RootPort
Max Age
Fwd Delay
Hello Time
Bridge
ID
Max Age
Hello
Fwd Delay
Force Version
Tx Hold Count
1 800000e052000100 0 800000e052000100 Root 20 15 2 800000e052000100 20 2 15 Default 3
RSTP Port
VLAN Port Priority Path Cost P2P Mac Edge Port Role State Designated Cost Designated Bridge
1 1/1/1 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/2 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/3 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/4 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/5 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/6 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/7 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/8 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/9 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/10 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/11 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/12 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/13 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/14 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/15 128 2000000 F F DESIGNATED FORWARDING 0 800000e052000100
1 1/1/23 128 0 F F DISABLED DISABLED 0 0000000000000000
1 1/1/24 128 2000000 F F DESIGNATED FORWARDING 0 800000e052000100
1 1/2/1 128 2000 F F DESIGNATED FORWARDING 0 800000e052000100
1 1/2/2 128 2000 F F DESIGNATED FORWARDING 0 800000e052000100
VLAN Port Priority Path Cost P2P Mac Edge Port Role State Designated Cost Designated Bridge
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 22 describes the fields in the RSTP window.

TABLE 22 Description of the fields in the RSTP window

Field	Description
RSTP Bridge parameters	
VLAN	Displays the port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all RSTP information is for VLAN 1.
RootBridge ID	Displays the ID of the root bridge that is associated with this bridge.
RootBridge PathCost	Displays the cumulative cost from this bridge to the root bridge. If this device is the root bridge, then the root cost is 0.
DesignateBridge ID	Displays the bridge from where the root information was received. It can be from the root bridge itself or from another bridge.
RootPort	Displays the port on this device that connects to the root bridge. If this device is the root bridge, then the value is **root** instead of a port number.
Max.Age	Displays the number of seconds this device or VLAN waits for a Hello message from the root bridge before deciding the root has become unavailable and performing a reconvergence.
Fwd Delay	Displays the number of seconds a non-edge designated port waits until it can apply any of the following transitions, if the received RST BPDU does not have an agreed flag: • Discarding state to learning state • Learning state to forwarding state When a non-edge port receives the RST BPDU, it goes into forwarding state within 4 seconds or after two hello timers expire on the port. Forward delay is also the number of seconds that a root port waits for an RST BPDU with a proposal flag before it applies the state transitions listed above. If the port is operating in 802.1D-compatible mode, then forward delay functionality is the same as in 802.1D (STP).
Hello Time	Displays the duration (secs) between two Hello packets.
Bridge ID	Displays the ID of the bridge.
Bridge Max Age	Displays the configured maximum age for this bridge. The default is 20.
Bridge Hello	Displays the configured hello time for this bridge.The default is 2.
Bridge Fwd Delay	Displays the configured forward delay time for this bridge. The default is 15.
Force Version	Displays the configured force version value, which can be one of the following: • **0** – The bridge has been forced to operate in an STP compatibility mode. • **2** – The bridge has been forced to operate in an RSTP mode. This is the default.
Tx Hold Count	Displays the number of BPDUs that can be transmitted per Hello interval. The default is 3.
RSTP Port parameters	
VLAN	Displays the port-based VLAN that owns the STP instance. VLAN 1 is the default VLAN. If you have not configured port-based VLANs on this device, all RSTP information is for VLAN 1.
Port	Displays the port number. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Priority	Displays the configured priority of the port. The default is 128 or 0x80.

TABLE 22 Description of the fields in the RSTP window (Continued)

Field	Description
Path Cost	Displays the configured path cost on a link connected to this port.
P2P Mac	Displays whether the point-to-point-MAC parameter is configured to be a point-to-point link: • **T** – The link is configured as a point-to-point link. • **F** – The link is not configured as a point-to-point link. This is the default.
Edge Port	Displays whether the port is configured as an operational edge port: • **T** – The port is configured as an edge port. • **F** – The port is not configured as an edge port. This is the default.
Role	Displays the current role of the port, which can be one of the following: • **ROOT** – Provides the lowest cost path to the root bridge from a specific bridge. • **DESIGNATED** – Provides the lowest cost path to the root bridge from a LAN to which it is connected. • **ALTERNATE** – Provides an alternate path to the root bridge when the root port goes down. • **BACKUP** – Provides a backup to the LAN when the Designated port goes down. • **DISABLED** – Has no role in the topology. For more information, refer to “Bridges and bridge port roles” of the *FastIron Configuration Guide*.
State	Displays the RSTP state of the port, which can be one of the following: • **DISCARDING** – RSTP has blocked data traffic on this port to prevent a loop. The device or VLAN can reach the root bridge using another port, whose state is FORWARDING. When a port is in this state, the port does not transmit or receive user frames, but the port does continue to receive STP BPDUs. This state corresponds to the listening and blocking states of 802.1D. • **DISABLED** – The port is not participating in RSTP. This can occur when the port is disconnected or STP is disabled on the port. • **FORWARDING** – RSTP is allowing the port to send and receive frames. • **LEARNING** – RSTP is allowing MAC entries to be added to the filtering database but does not permit forwarding of data frames. The device can learn the MAC addresses of frames that the port receives during this state and make corresponding entries in the MAC table.
Designated Cost	Displays the best root path cost that this port received, including the best root path cost that it can transmit.
Designated Bridge	Displays the ID of the bridge that sent the best RST BPDU that was received on this port.

Chapter

7

Monitoring IP

In this chapter

- Displaying IP cache 59
- Displaying IP traffic information for devices running Layer 2 code 60
- Displaying IP traffic information for devices running Layer 3 code 64
- Displaying the IP routing table 66

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

Displaying IP cache

NOTE
The IP cache is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

To display the IP forwarding cache information, perform the following steps.

1. Click **Monitor** on the left pane and select **IP**.
2. Click **Cache**.

The **IP Cache** window is displayed as shown in Figure 36.

FIGURE 36 Monitoring the IP cache

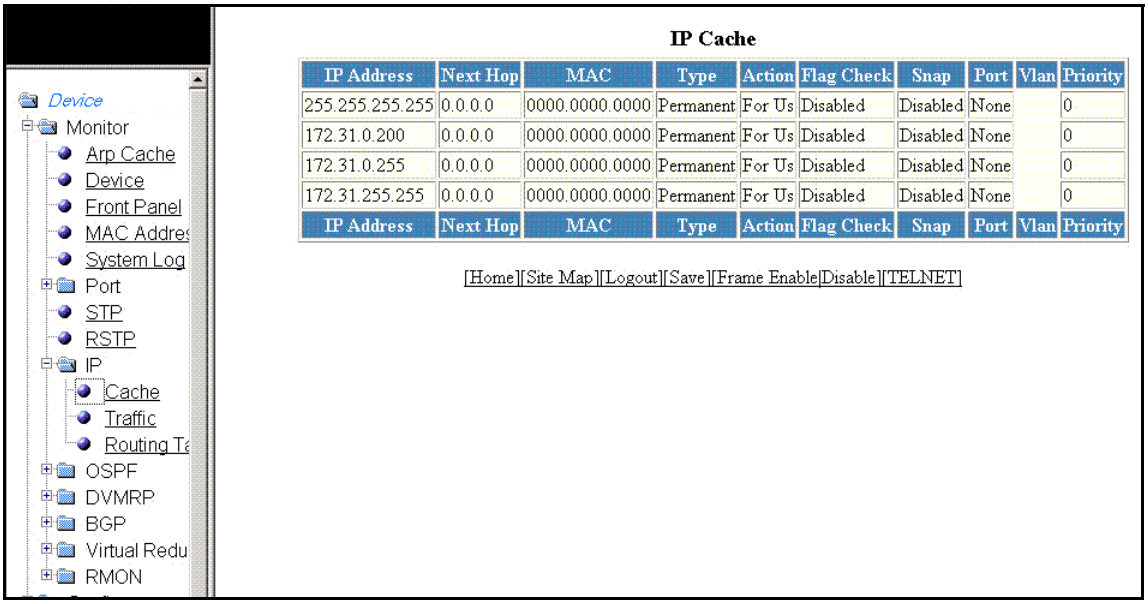


Table 23 describes the fields in the **IP Cache** window.

TABLE 23 Description of the fields in the **IP Cache** window

Field	Description
IP Address	Displays the IP address of the destination.
Next Hop	Displays the IP address of the next hop router to the destination. This field contains either an IP address or the value DIRECT. DIRECT means the destination is either directly attached or the destination is an address on this Brocade device.
MAC	Displays the MAC address of the destination. **NOTE:** If the entry is type Us (indicating that the destination is this Brocade device), the address consists of zeroes.
Type	Displays the type of host entry, which can be one of the following: • **Dynamic** • **Permanent** • **Forward** • **Us** • **Complex Filter** • **Wait ARP** • **ICMP Deny** • **Drop** • **Fragment** • **Snap Encap**
Action	Displays the action the router takes for the packet.
Flag Check	Displays whether the flag check has been enabled or disabled.
Snap	Displays whether the snap encapsulation has been enabled or disabled.
Port	Displays the port through which this device reaches the destination. For destinations that are located on this device, the port number is shown as “n/a”.
Vlan	Displays the VLAN the port is in.
Priority	Displays the Quality of Service (QoS) priority of the port or the VLAN.

Displaying IP traffic information for devices running Layer 2 code

To display the IP traffic statistics for Brocade FCX, Brocade ICX 6610, and Brocade FSX devices running Layer 2 code, perform the following steps.

1. Click **Monitor** on the left pane and select **IP**.
2. Click **Traffic**.

The **IP Traffic** window is displayed as shown in Figure 37.

FIGURE 37 Monitoring the IP traffic for devices running Layer 2 code

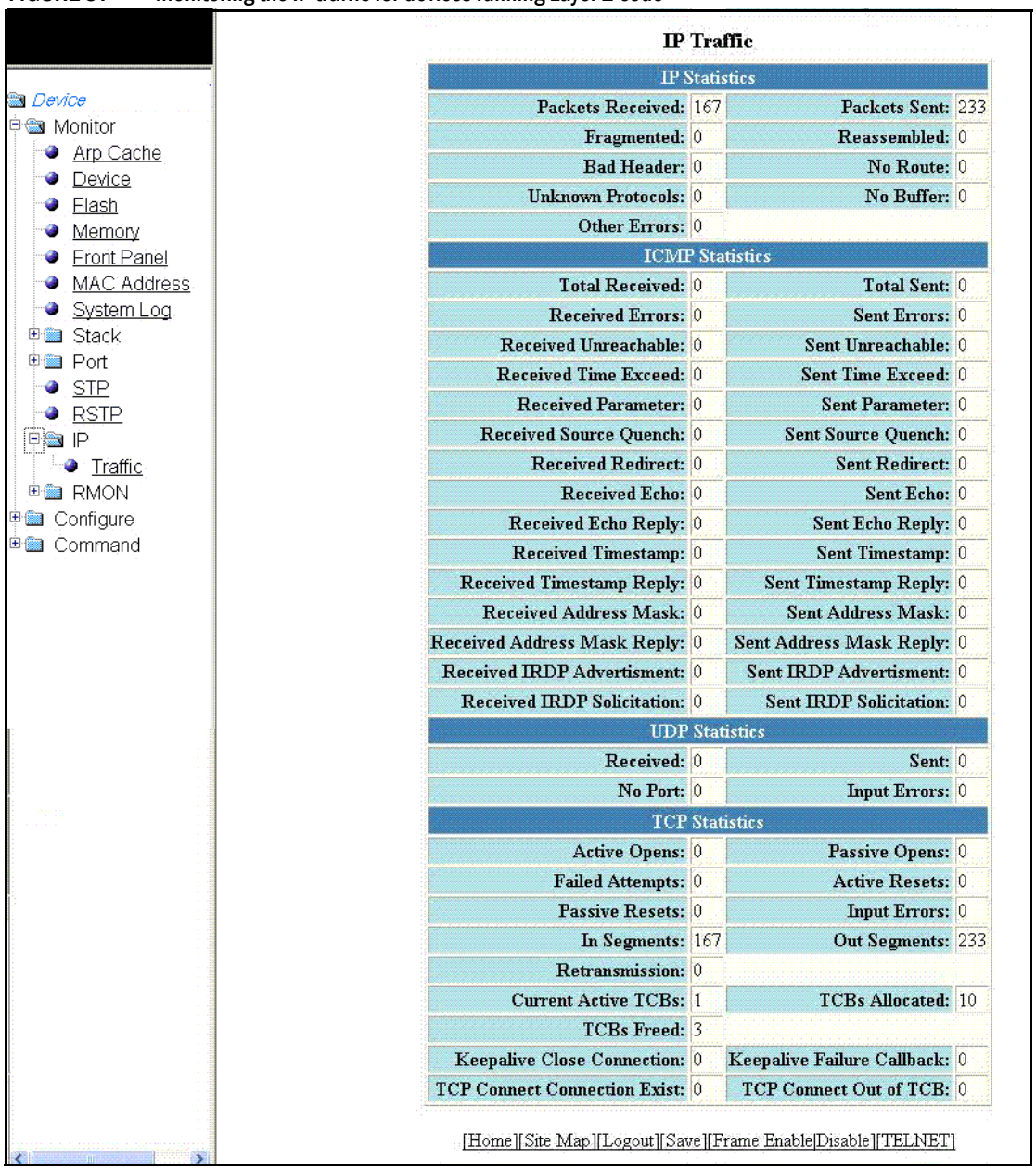


Table 24 describes the fields in the **IP Traffic** window.

TABLE 24 Description of the fields in the **IP Traffic** window

Field	Description
IP Statistics parameters	
Packets Received	Displays the number of IP packets received by the device.
Packets Sent	Displays the number of IP packets originated and sent by the device.
Fragmented	Displays the number of IP packets fragmented by this device before sending or forwarding them.

TABLE 24 Description of the fields in the **IP Traffic** window (Continued)

Field	Description
Reassembled	Displays the number of fragmented IP packets received and re-assembled by the device.
Bad Header	Displays the number of IP packets dropped because they had a bad header.
No Route	Displays the number of packets dropped by the device because they had no route information.
Unknown Protocols	Displays the number of packets dropped by the device because the value in the protocol field of the packet header is unrecognized by this device.
No Buffer	Displays the number of packets dropped because the device ran out of buffer space.
Other Errors	Displays the number of packets dropped due to errors other than the ones already indicated in the **IP Statistics** parameters.
ICMP Statistics parameters	
Total Received	Displays the number of Internet Control Message Protocol (ICMP) packets received by the device.
Total Sent	Displays the number of ICMP packets sent by the device.
Received Errors	Displays the number of errors received by the device. This information is used by Brocade customer support.
Sent Errors	Displays the number of errors sent by the device. This information is used by Brocade customer support.
Received Unreachable	Displays the number of Destination Unreachable messages received by the device.
Sent Unreachable	Displays the number of Destination Unreachable messages sent by the device.
Received Time Exceed	Displays the number of Time Exceeded messages received by the device.
Sent Time Exceed	Displays the number of Time Exceeded messages sent by the device.
Received Parameter	Displays the number of Parameter Problem messages received by the device.
Sent Parameter	Displays the number of Parameter Problem messages sent by the device.
Received Source Quench	Displays the number of Source Quench messages received by the device.
Sent Source Quench	Displays the number of Source Quench messages sent by the device.
Received Redirect	Displays the number of Redirect messages received by the device.
Sent Redirect	Displays the number of Redirect messages sent by the device.
Received Echo	Displays the number of Echo messages received by the device.
Sent Echo	Displays the number of Echo messages sent by the device.
Received Echo Reply	Displays the number of Echo Reply messages received by the device.
Sent Echo Reply	Displays the number of Echo Reply messages sent by the device.
Received Timestamp	Displays the number of Timestamp messages received by the device.
Sent Timestamp	Displays the number of Timestamp messages sent by the device.
Received Timestamp Reply	Displays the number of Timestamp Reply messages received by the device.
Sent Timestamp Reply	Displays the number of Timestamp Reply messages sent by the device.
Received Address Mask	Displays the number of Address Mask Request messages received by the device.

TABLE 24 Description of the fields in the **IP Traffic** window (Continued)

Field	Description
Sent Address Mask	Displays the number of Address Mask Request messages sent by the device.
Received Address Mask Reply	Displays the number of Address Mask Reply messages received by the device.
Sent Address Mask Reply	Displays the number of Address Mask Reply messages sent by the device.
Received IRDP Advertisement	Displays the number of ICMP Router Discovery Protocol (IRDP) Advertisement messages received by the device.
Sent IRDP Advertisement	Displays the number of IRDP Advertisement messages sent by the device.
Received IRDP Solicitation	Displays the number of IRDP Solicitation messages received by the device.
Sent IRDP Solicitation	Displays the number of IRDP Solicitation messages sent by the device.
UDP Statistics parameters	
Received	Displays the number of User Datagram Protocol (UDP) packets received by the device.
Sent	Displays the number of UDP packets sent by the device.
No Port	Displays the number of UDP packets dropped because the packet did not contain a valid UDP port number.
Input Errors	Displays the number of errors on the incoming packets. This information is used by Brocade customer support.
TCP Statistics parameters	
Active Opens	Displays the number of Transmission Control Protocol (TCP) connections opened by this device by sending a TCP SYN to another device.
Passive Opens	Displays the number of TCP connections opened by this device in response to connection requests (TCP SYNs) received from other devices.
Failed Attempts	Displays the number of failed attempts. This information is used by Brocade customer support.
Active Resets	Displays the number of TCP connections this device reset by sending a TCP RESET message to the device at the other end of the connection.
Passive Resets	Displays the number of TCP connections this device reset because the device at the other end of the connection sent a TCP RESET message.
Input Errors	Displays the number of incoming errors. This information is used by Brocade customer support.
In Segments	Displays the number of TCP segments received by the device.
Out Segments	Displays the number of TCP segments sent by the device.
Retransmission	Displays the number of segments that this device retransmitted because the retransmission timer for the segment had expired before the device at the other end of the connection had acknowledged receipt of the segment.
Current Active TCBs	Displays the number of TCP Control Blocks (TCBs) that are currently active.
TCBs Allocated	Displays the number of TCBs that have been allocated.
TCBs Freed	Displays the number of TCBs that have been freed.

Displaying IP traffic information for devices running Layer 3 code

To display the IP traffic statistics for Brocade FCX, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code, perform the following steps.

1. Click **Monitor** on the left pane and select **IP**.
2. Click **Traffic**.

The **IP Traffic** window is displayed as shown in Figure 38.

FIGURE 38 Monitoring the IP traffic information for devices running Layer 3 code

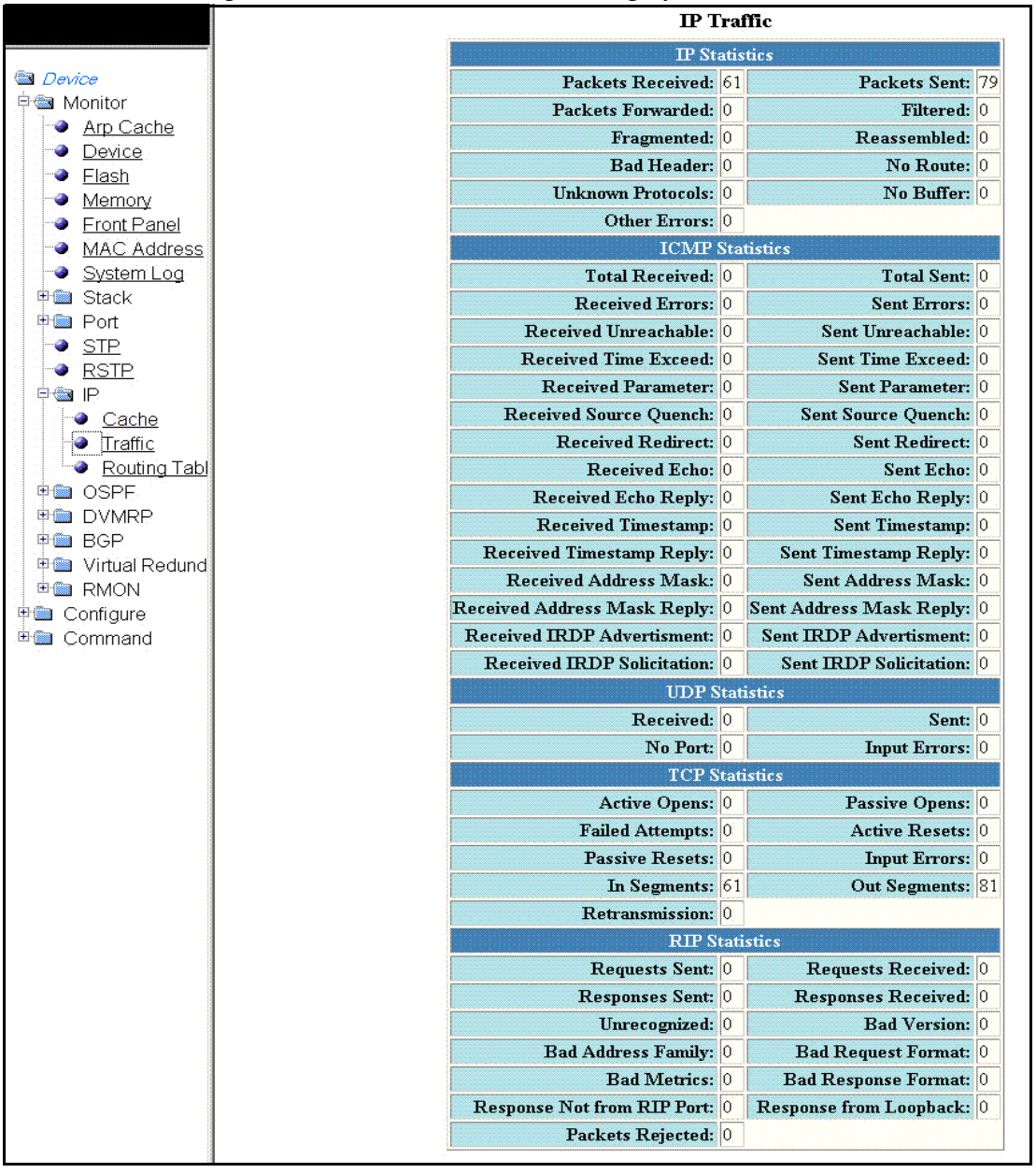


Table 25 describes the fields in the **IP Traffic** window.

TABLE 25 Description of the fields in the **IP Traffic** window

Field	Description
IP Statistics parameters	
Packets Received	Displays the number of IP packets received by the device.
Packets Sent	Displays the number of IP packets originated and sent by the device.
Packets Forwarded	Displays the total number of IP packets received by the device and forwarded to other devices.
Filtered	Displays the total number of IP packets filtered by the device.
Fragmented	Displays the number of IP packets fragmented by this device before sending or forwarding them.
Reassembled	Displays the number of fragmented IP packets received and re-assembled by the device.
Bad Header	Displays the number of IP packets dropped because they had a bad header.
No Route	Displays the number of packets dropped by the device because they had no route information.
Unknown Protocols	Displays the number of packets dropped by the device because the value in the protocol field of the packet header is unrecognized by this device.
No Buffer	Displays the number of packets dropped because the device ran out of buffer space.
Other Errors	Displays the number of packets dropped due to errors other than the ones already indicated in the **IP Statistics** parameters.
ICMP Statistics	Refer to "ICMP Statistics parameters" on page 62.
UDP Statistics	Refer to "UDP Statistics parameters" on page 63.
TCP Statistics parameters	
Active Opens	Displays the number of TCP connections opened by this device by sending a TCP SYN to another device.
Passive Opens	Displays the number of TCP connections opened by this device in response to connection requests (TCP SYNs) received from other devices.
Failed Attempts	Displays the number of failed attempts. This information is used by Brocade customer support.
Active Resets	Displays the number of TCP connections this device reset by sending a TCP RESET message to the device at the other end of the connection.
Passive Resets	Displays the number of TCP connections this device reset because the device at the other end of the connection sent a TCP RESET message.
Input Errors	Displays the number of incoming errors. This information is used by Brocade customer support.
In Segments	Displays the number of TCP segments received by the device.
Out Segments	Displays the number of TCP segments sent by the device.
Retransmission	Displays the number of segments that this device retransmitted because the retransmission timer for the segment had expired before the device at the other end of the connection had acknowledged receipt of the segment.

TABLE 25 Description of the fields in the **IP Traffic** window (Continued)

Field	Description
RIP Statistics parameters	
Requests Sent	Displays the number of requests this device has sent to another Routing Information Protocol (RIP) Layer 3 switch for all or part of its RIP routing table.
Requests Received	Displays the number of requests this device has received from another RIP Layer 3 switch for all or part of this device's RIP routing table.
Responses Sent	Displays the number of responses this device has sent to another RIP Layer 3 switch's request for all or part of this device's RIP routing table.
Responses Received	Displays the number of responses this device has received to requests for all or part of another RIP Layer 3 switch's routing table.
Unrecognized	Displays the number of RIP packets that were not recognized by the device.
Bad Version	Displays the number of RIP packets dropped by the device because the RIP version was either invalid or is not supported by this device.
Bad Address Family	Displays the number of RIP packets dropped because the value in the Address Family Identifier field of the packet's header was invalid.
Bad Request Format	Displays the number of RIP request packets this Layer 3 switch dropped because the format was bad.
Bad Metrics	Displays the number of responses to RIP request packets this Layer 3 switch dropped because of the bad metric value. This information is used by Brocade customer support.
Bad Response Format	Displays the number of responses to RIP request packets this Layer 3 switch dropped because the format was bad.
Response Not from RIP Port	Displays the number of RIP responses received from non-RIP ports. This information is used by Brocade customer support.
Response from Loopback	Displays the number of RIP responses received from loopback interfaces.
Packets Rejected	Displays the number of RIP packets rejected by the device.

Displaying the IP routing table

NOTE
The IP routing table is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

To display the IP routing table information, perform the following steps.

1. Click **Monitor** on the left pane and select **IP**.
2. Click **Routing Table**.

The **Routing Table** window is displayed as shown in Figure 39.

FIGURE 39 Monitoring the IP routing table

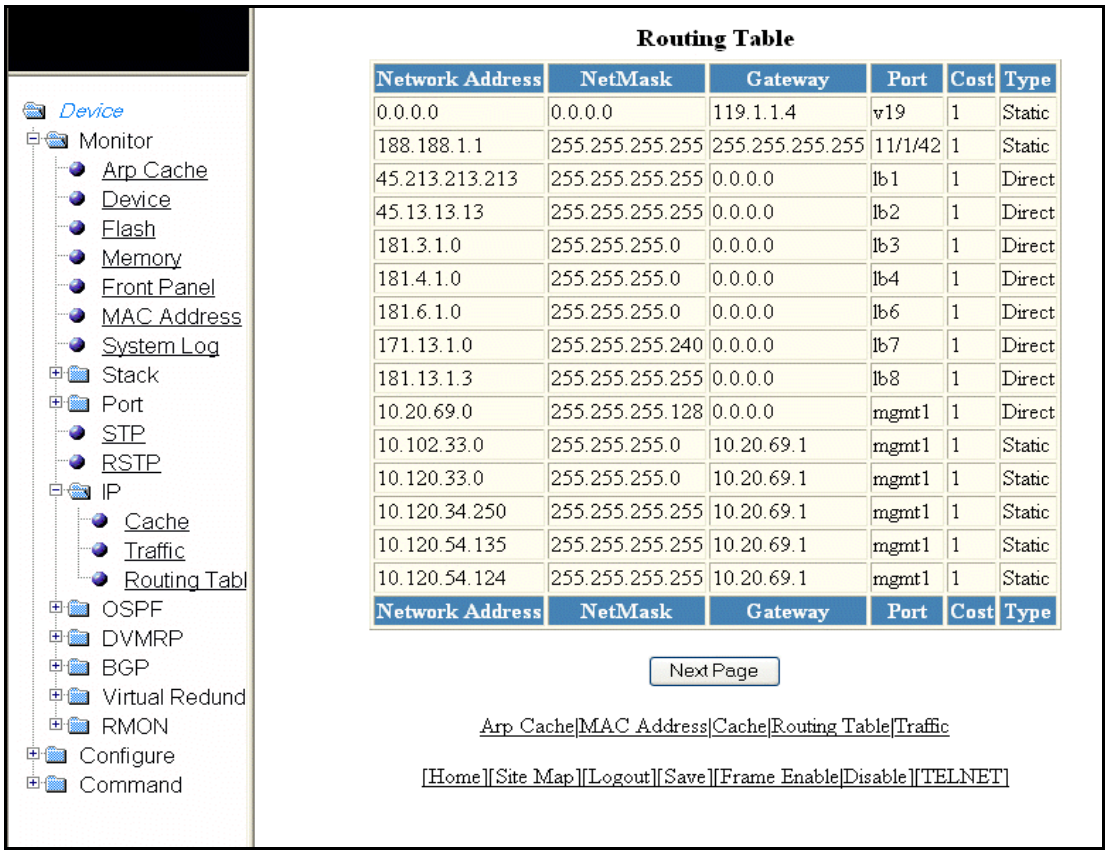


Table 26 describes the fields in the **Routing Table** window.

TABLE 26 Description of the fields in the **Routing Table** window

Field	Description
Network Address	Displays the destination network address of the route.
NetMask	Displays the network mask of the destination address.
Gateway	Displays the IP address of the next hop router.
Port	Displays the port through which this Layer 3 switch sends packets to reach the destination of the route.
Cost	Displays the cost of the route.
Type	Displays the route type, which can be one of the following: • **Direct** – The destination is directly connected to this Layer 3 switch. • **Static** – The route is a static route. • **BGP** - The route was learned from BGP. • **RIP** - The route was learned from RIP. • **OSPF** - The route is an OSPF route.

7 Displaying the IP routing table

Chapter

Monitoring OSPF

8

In this chapter

- Displaying the OSPF ABR ASBR router information 69
- Displaying OSPF area information 71
- Displaying OSPF external link-state database 73
- Displaying the OSPF interfaces 75
- Displaying OSPF link state database 78
- Displaying OSPF neighbors 80
- Displaying OSPF virtual interfaces 82
- Displaying OSPF virtual neighbors 85

NOTE
The Open Shortest Path First (OSPF) feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

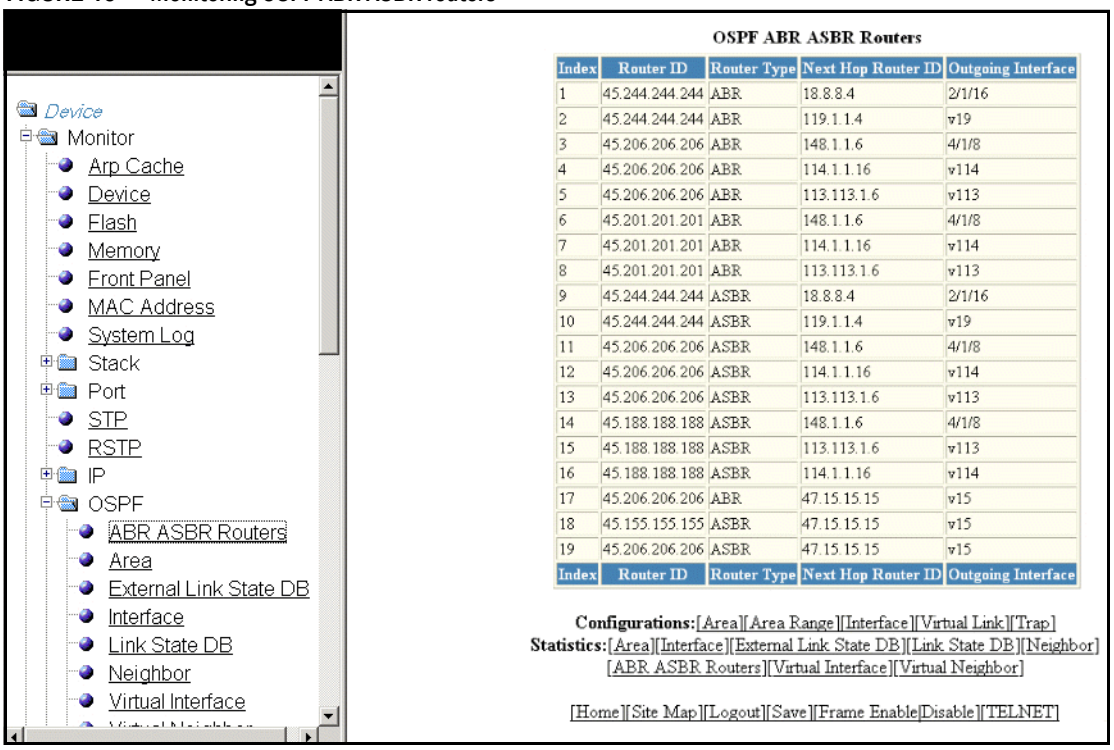
Displaying the OSPF ABR ASBR router information

To display the Open Shortest Path First (OSPF) Area Border Router (ABR) Autonomous System Boundary Router (ASBR) information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **ABR ASBR Routers**.

The **OSPF ABR ASBR Routers** window is displayed as shown in Figure 40.

FIGURE 40 Monitoring OSPF ABR ASBR routers



Index	Router ID	Router Type	Next Hop Router ID	Outgoing Interface
1	45.244.244.244	ABR	18.8.8.4	2/1/16
2	45.244.244.244	ABR	119.1.1.4	v19
3	45.206.206.206	ABR	148.1.1.6	4/1/8
4	45.206.206.206	ABR	114.1.1.16	v114
5	45.206.206.206	ABR	113.113.1.6	v113
6	45.201.201.201	ABR	148.1.1.6	4/1/8
7	45.201.201.201	ABR	114.1.1.16	v114
8	45.201.201.201	ABR	113.113.1.6	v113
9	45.244.244.244	ASBR	18.8.8.4	2/1/16
10	45.244.244.244	ASBR	119.1.1.4	v19
11	45.206.206.206	ASBR	148.1.1.6	4/1/8
12	45.206.206.206	ASBR	114.1.1.16	v114
13	45.206.206.206	ASBR	113.113.1.6	v113
14	45.188.188.188	ASBR	148.1.1.6	4/1/8
15	45.188.188.188	ASBR	113.113.1.6	v113
16	45.188.188.188	ASBR	114.1.1.16	v114
17	45.206.206.206	ABR	47.15.15.15	v15
18	45.155.155.155	ASBR	47.15.15.15	v15
19	45.206.206.206	ASBR	47.15.15.15	v15

Table 27 describes the fields in the **OSPF ABR ASBR Routers** window.

TABLE 27 Description of the fields in the **OSPF ABR ASBR Routers** window

Field	Description
Index	Displays the row number of the entry in the OSPF ABR ASBR Routers table.
Router ID	Displays the IP address of the neighbor router.
Router Type	Displays the router type, which can be one of the following: • **ABR** – Indicates that the OSPF router is a member of multiple areas. • **ASBR** – Indicates that the router is running multiple protocols and serves as a gateway to routers outside an area and those operating with different protocols.
Next Hop Router ID	Displays the IP address of the next hop router.
Outgoing Interface	Displays the Layer 3 switch interface through which a packet must traverse to reach the next hop router.

The **OSPF ABR ASBR Routers** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.

  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Displaying OSPF area information

To display OSPF area information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **Area**.

The **OSPF Area** window is displayed as shown in Figure 41.

FIGURE 41 Monitoring the OSPF area

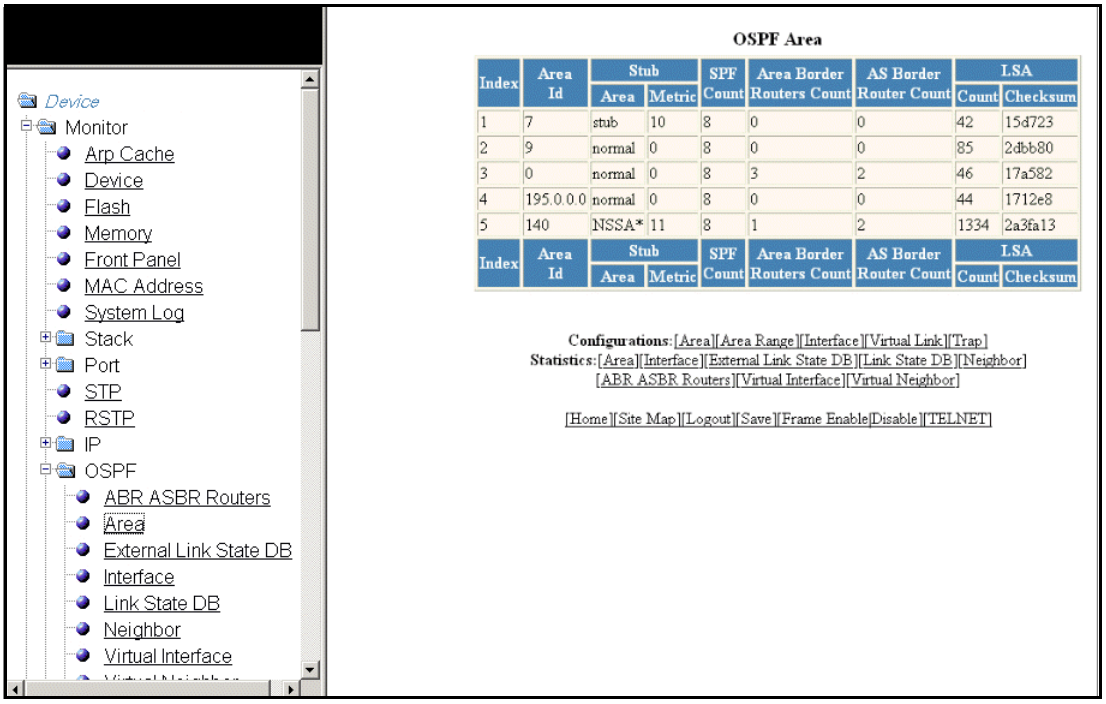


Table 28 describes the fields in the **OSPF Area** window.

TABLE 28 Description of the fields in the **OSPF Area** window

Field	Description
Index	Displays the row number of the entry in the OSPF Area table.
Area Id	Displays the area number.
Stub	• **Area** – Displays the area type, which can be one of the following: - NSSA - normal - stub • **Metric** – Displays the area cost.
SPF Count	The cost of traversing the Shortest Path First (SPF) node to reach the destination.
Area Border Routers Count	Displays the ABR number.
AS Border Router Count	Displays the ASBR number.
LSA	• **Count** – Displays the Link-State Advertisement (LSA) number. • **Checksum** – Displays the checksum for the LSA packet. The checksum is based on all the fields in the packet except the age field.

The **OSPF Area** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.

  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Displaying OSPF external link-state database

To display the OSPF external link-state database information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **External Link State DB**.

The **OSPF External Link State DB** window is displayed as shown in Figure 42.

FIGURE 42 Monitoring the OSPF external link-state DB

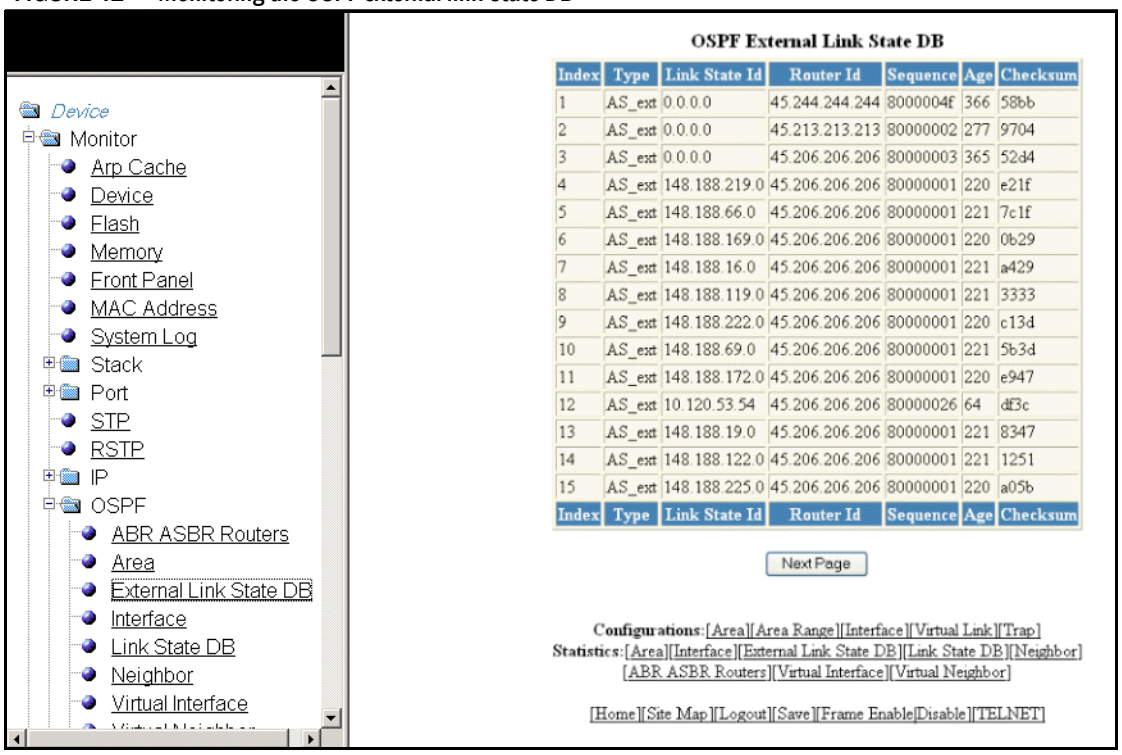

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Address
System Log
Stack
Port
STP
RSTP
IP
OSPF
ABR ASBR Routers
Area
External Link State DB
Interface
Link State DB
Neighbor
Virtual Interface
OSPF External Link State DB
Index Type Link State Id Router Id Sequence Age Checksum
1 AS_ext 0.0.0.0 45.244.244.244 8000004f 366 58bb
2 AS_ext 0.0.0.0 45.213.213.213 80000002 277 9704
3 AS_ext 0.0.0.0 45.206.206.206 80000003 365 52d4
4 AS_ext 148.188.219.0 45.206.206.206 80000001 220 e21f
5 AS_ext 148.188.66.0 45.206.206.206 80000001 221 7c1f
6 AS_ext 148.188.169.0 45.206.206.206 80000001 220 0b29
7 AS_ext 148.188.16.0 45.206.206.206 80000001 221 a429
8 AS_ext 148.188.119.0 45.206.206.206 80000001 221 3333
9 AS_ext 148.188.222.0 45.206.206.206 80000001 220 c13d
10 AS_ext 148.188.69.0 45.206.206.206 80000001 221 5b3d
11 AS_ext 148.188.172.0 45.206.206.206 80000001 220 e947
12 AS_ext 10.120.53.54 45.206.206.206 80000026 64 df3c
13 AS_ext 148.188.19.0 45.206.206.206 80000001 221 8347
14 AS_ext 148.188.122.0 45.206.206.206 80000001 221 1251
15 AS_ext 148.188.225.0 45.206.206.206 80000001 220 a05b
Index Type Link State Id Router Id Sequence Age Checksum
Next Page
Configurations:[Area][Area Range][Interface][Virtual Link][Trap]
Statistics:[Area][Interface][External Link State DB][Link State DB][Neighbor]
[ABR ASBR Routers][Virtual Interface][Virtual Neighbor]
[Home][Site Map][Logout][Save][Frame Enable][Disable][TELNET]

Table 29 describes the fields in the **OSPF External Link State DB** window.

TABLE 29 Description of the fields in the **OSPF External Link State DB** window

Field	Description
Index	Displays the row number of the entry in the OSPF External Link State DB table.
Type	Displays the route type, which is always **As_ext**.
Link State Id	Displays the Identifier of the link-state advertisement from which the Layer 3 switch learned this route.
Router Id	Displays the IP address of the Layer 3 switch.
Sequence	Displays the sequence number of the LSA. The OSPF neighbor that sent the LSA stamps it with a sequence number to enable the Layer 3 switch and other OSPF routers to determine which LSA for a given route is the most recent.
Age	Displays the age of the LSA, in seconds.
Checksum	Displays the checksum for the LSA packet, which is based on all the fields in the packet except the age field. The Layer 3 switch uses the checksum to verify that the packet is not corrupted.

The **OSPF External Link State DB** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.

  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

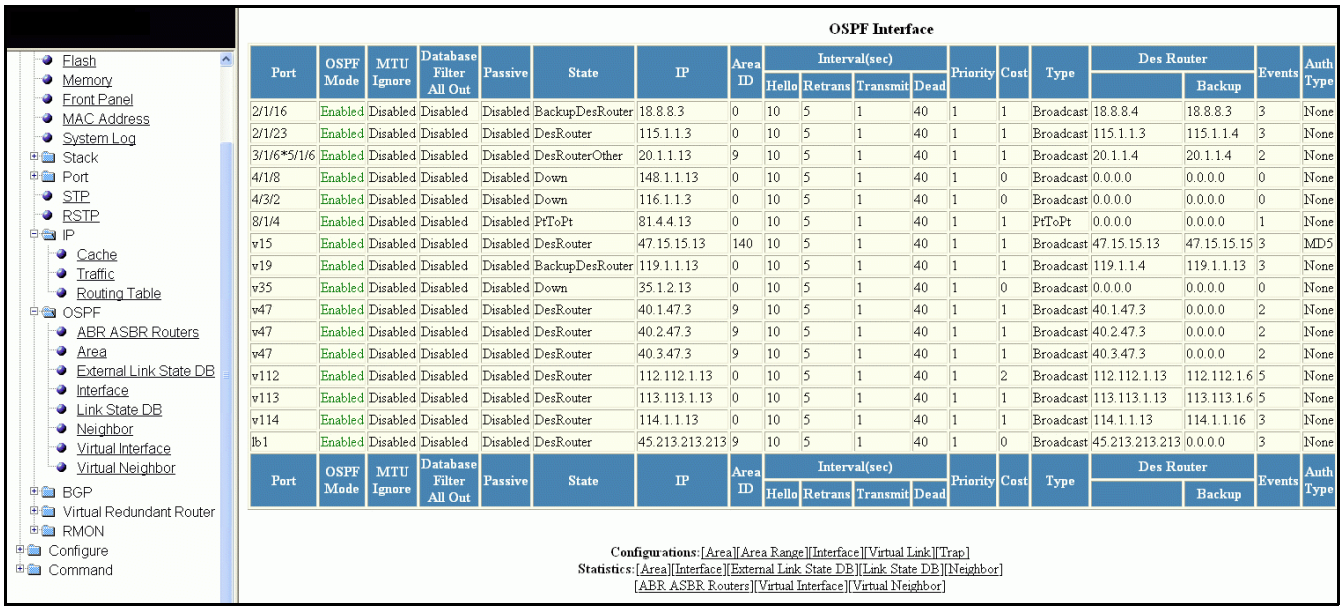
Displaying the OSPF interfaces

To display the OSPF interface information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **Interface**.

The **OSPF Interface** window is displayed as shown in Figure 43.

FIGURE 43 Monitoring OSPF interfaces



OSPF Interface

Port	OSPF Mode	MTU Ignore	Database Filter All Out	Passive	State	IP	Area ID	Interval(sec)				Priority	Cost	Type	Des Router		Events	Auth Type
								Hello	Retrans	Transmit	Dead					Backup		
2/1/16	Enabled	Disabled	Disabled	Disabled	BackupDesRouter	18.8.8.3	0	10	5	1	40	1	1	Broadcast	18.8.8.4	18.8.8.3	3	None
2/1/23	Enabled	Disabled	Disabled	Disabled	DesRouter	115.1.1.3	0	10	5	1	40	1	1	Broadcast	115.1.1.3	115.1.1.4	3	None
3/1/6*5/1/6	Enabled	Disabled	Disabled	Disabled	DesRouterOther	20.1.1.13	9	10	5	1	40	1	1	Broadcast	20.1.1.4	20.1.1.4	2	None
4/1/8	Enabled	Disabled	Disabled	Disabled	Down	148.1.1.13	0	10	5	1	40	1	0	Broadcast	0.0.0.0	0.0.0.0	0	None
4/3/2	Enabled	Disabled	Disabled	Disabled	Down	116.1.1.3	0	10	5	1	40	1	0	Broadcast	0.0.0.0	0.0.0.0	0	None
8/1/4	Enabled	Disabled	Disabled	Disabled	PtToPt	81.4.4.13	0	10	5	1	40	1	1	PtToPt	0.0.0.0	0.0.0.0	1	None
v15	Enabled	Disabled	Disabled	Disabled	DesRouter	47.15.15.13	140	10	5	1	40	1	1	Broadcast	47.15.15.13	47.15.15.15	3	MD5
v19	Enabled	Disabled	Disabled	Disabled	BackupDesRouter	119.1.1.13	0	10	5	1	40	1	1	Broadcast	119.1.1.4	119.1.1.13	3	None
v35	Enabled	Disabled	Disabled	Disabled	Down	35.1.2.13	0	10	5	1	40	1	0	Broadcast	0.0.0.0	0.0.0.0	0	None
v47	Enabled	Disabled	Disabled	Disabled	DesRouter	40.1.47.3	9	10	5	1	40	1	1	Broadcast	40.1.47.3	0.0.0.0	2	None
v47	Enabled	Disabled	Disabled	Disabled	DesRouter	40.2.47.3	9	10	5	1	40	1	1	Broadcast	40.2.47.3	0.0.0.0	2	None
v47	Enabled	Disabled	Disabled	Disabled	DesRouter	40.3.47.3	9	10	5	1	40	1	1	Broadcast	40.3.47.3	0.0.0.0	2	None
v112	Enabled	Disabled	Disabled	Disabled	DesRouter	112.112.1.13	0	10	5	1	40	1	2	Broadcast	112.112.1.13	112.112.1.6	5	None
v113	Enabled	Disabled	Disabled	Disabled	DesRouter	113.113.1.13	0	10	5	1	40	1	1	Broadcast	113.113.1.13	113.113.1.6	5	None
v114	Enabled	Disabled	Disabled	Disabled	DesRouter	114.1.1.13	0	10	5	1	40	1	1	Broadcast	114.1.1.13	114.1.1.16	3	None
lb1	Enabled	Disabled	Disabled	Disabled	DesRouter	45.213.213.213	9	10	5	1	40	1	0	Broadcast	45.213.213.213	0.0.0.0	3	None
Port	OSPF Mode	MTU Ignore	Database Filter All Out	Passive	State	IP	Area ID	Interval(sec)				Priority	Cost	Type	Des Router		Events	Auth Type
								Hello	Retrans	Transmit	Dead					Backup		

Configurations: [Area] [Area Range] [Interface] [Virtual Link] [Trap]
Statistics: [Area] [Interface] [External Link State DB] [Link State DB] [Neighbor]
[ABR ASBR Routers] [Virtual Interface] [Virtual Neighbor]

Table 30 describes the fields in the **OSPF Interface** window.

TABLE 30 Description of the fields in the **OSPF Interface** window

Field	Description
Port	Displays the port number for which the OSPF interface data is being presented. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
OSPF Mode	Displays whether the OSPF mode is enabled.
MTU Ignore	Displays whether the mismatch detection that verifies if the same maximum transmission unit (MTU) is used on an interface shared by neighbors is enabled. By default, it is enabled.
Database Filter All Out	Displays whether the filter to an OSPF interface to block flooding of outbound LSAs on the interface is enabled.
Passive	Displays whether an OSPF interface is enabled to be passive. When you configure an OSPF interface to be passive, that interface does not send or receive OSPF route updates.
State	Displays the state of the interface, which can be one of the following: • **DesRouter** – The interface is functioning as the Designated Router (DR) for OSPF. • **BackupDesRouter** – The interface is functioning as the Backup Designated Router (BDR) for OSPF. • **Loopback** – The interface is functioning as a loopback interface. • **PtToPt** – The interface is functioning as a point-to-point interface. • **Passive** – The interface is up but it does not take part in forming an adjacency. • **Waiting** – The interface is trying to determine the identity of the BDR for the network. • **None** – The interface does not take part in the OSPF interface state machine.

TABLE 30 Description of the fields in the **OSPF Interface** window (Continued)

Field	Description
State (continued)	• **Down** – The interface is unusable. No protocol traffic can be sent or received on such an interface. • **DesRouter other** – The interface is a broadcast or Non-Broadcast Multi-Access (NBMA) network on which another Layer 3 switch is selected to be the DR.
IP	Displays the IP address assigned to the interface.
Area ID	Displays the value of the area in which the interface belongs.
Interval (sec)	Displays the interval, in seconds, of the hello-interval, dead-interval, and retransmit-interval timers.
Priority	Displays the priority used when selecting the DR and the BDR. If the priority is 0, the interface does not participate in the DR and BDR election.
Cost	Displays the overhead required to send a packet through the interface.
Type	Displays the type of OSPF circuit running on the interface, which can be one of the following: • **Broadcast** • **PtToPt**
Des Router	Displays the router IP address of the designated router.
Events	Displays the OSPF interface event, which can be one of the following: • **0** - Interface Up • **1** - Wait Timer • **2** - Backup Seen • **3** - Neighbor Change • **4** - Loop Indication • **5** - Unloop Indication • **6** - Interface Down • **7** - Interface Passive
Auth Type	Displays the type of authentication, which can be one of the following: • **MD5** • **None** • **Simple Password**
Simple Auth Key	Dispalys the simple authentication key.
MD5 Auth	Displays the MD5 key that is being used.

The **OSPF Interface** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.

- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Displaying OSPF link state database

To display the link state database information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **Link State DB**.

The **OSPF Link State DB** window is displayed as shown in Figure 44.

FIGURE 44 Monitoring the OSPF link state DB

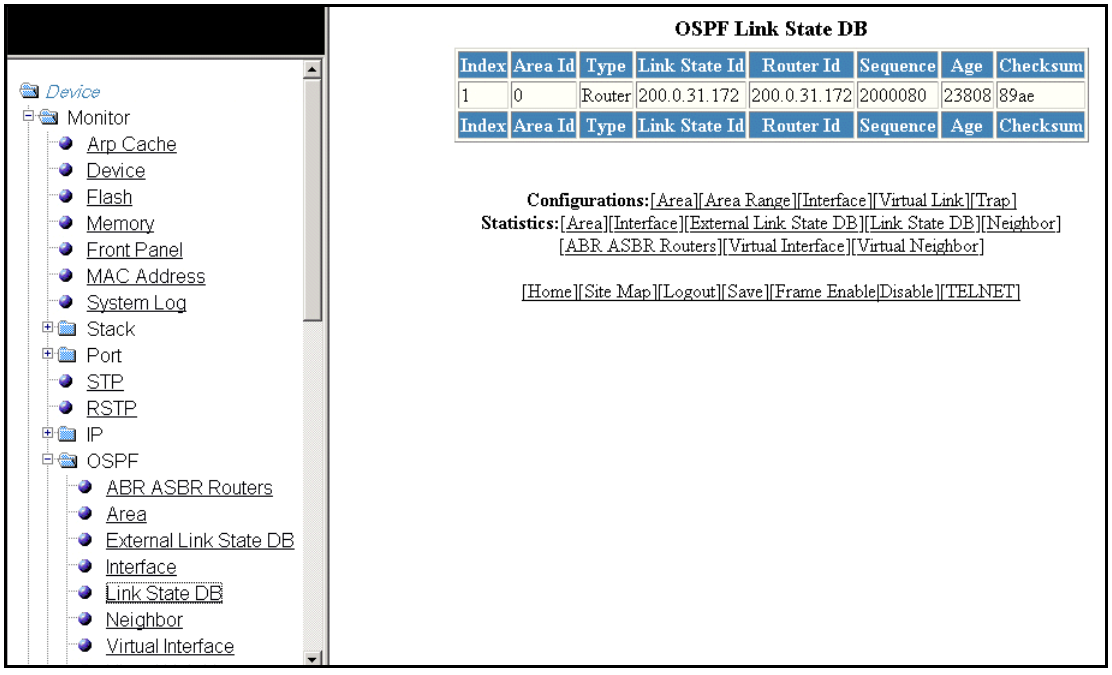


Table 31 describes the fields in the **OSPF Link State DB** window.

TABLE 31 Description of the fields in the **OSPF Link State DB** window

Field	Description
Index	Displays the row number of the entry in the OSPF Link State table.
Area Id	Displays the area number.
Type	Displays the type of LSA, which can be one of the following: • **Router** • **Network** • **Inter-area prefix** • **Inter-area router** • **AS external** • **Link** • **Intra-area prefix** • **Summary**
Link State Id	Displays the ID of the LSA from which the Layer 3 switch learned this route.
Router Id	Displays the External LSAs for the specified OSPF Layer 3 switch.
Sequence	Displays the sequence number of the LSA. The OSPF neighbor that sent the LSA stamps it with a sequence number to enable the Layer 3 switch and other OSPF Layer 3 switches to determine which LSA for a given route is the most recent.
Age	Displays the age of the LSA, in seconds.
Checksum	Displays the checksum for the LSA packet, which is based on all the fields in the packet except the age field. The Layer 3 switch uses the checksum to verify that the packet is not corrupted.

The **OSPF Link State DB** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.

- To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
- To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
- To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
- To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Displaying OSPF neighbors

To display the OSPF neighbor information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **Neighbor**.

The **OSPF Neighbor** window is displayed as shown in Figure 45.

FIGURE 45 Monitoring OSPF neighbors

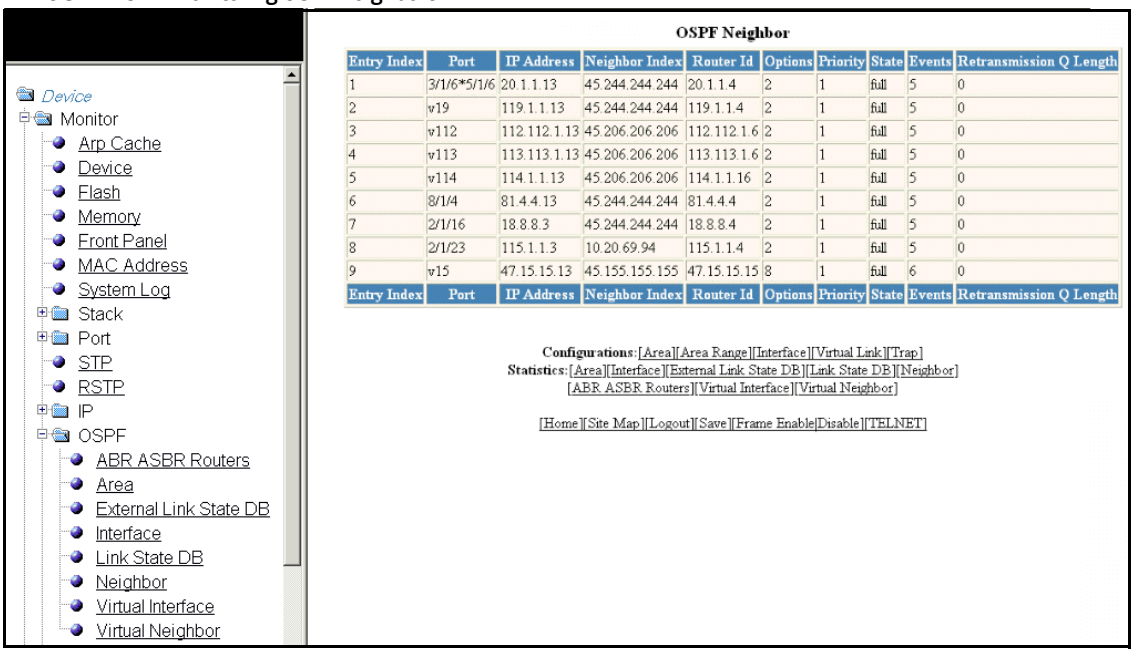

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Address
System Log
Stack
Port
STP
RSTP
IP
OSPF
ABR ASBR Routers
Area
External Link State DB
Interface
Link State DB
Neighbor
Virtual Interface
Virtual Neighbor
OSPF Neighbor
Entry Index | Port | IP Address | Neighbor Index | Router Id | Options | Priority | State | Events | Retransmission Q Length
1 | 3/1/6*5/1/6 | 20.1.1.13 | 45.244.244.244 | 20.1.1.4 | 2 | 1 | full | 5 | 0
2 | v19 | 119.1.1.13 | 45.244.244.244 | 119.1.1.4 | 2 | 1 | full | 5 | 0
3 | v112 | 112.112.1.13 | 45.206.206.206 | 112.112.1.6 | 2 | 1 | full | 5 | 0
4 | v113 | 113.113.1.13 | 45.206.206.206 | 113.113.1.6 | 2 | 1 | full | 5 | 0
5 | v114 | 114.1.1.13 | 45.206.206.206 | 114.1.1.16 | 2 | 1 | full | 5 | 0
6 | 8/1/4 | 81.4.4.13 | 45.244.244.244 | 81.4.4.4 | 2 | 1 | full | 5 | 0
7 | 2/1/16 | 18.8.8.3 | 45.244.244.244 | 18.8.8.4 | 2 | 1 | full | 5 | 0
8 | 2/1/23 | 115.1.1.3 | 10.20.69.94 | 115.1.1.4 | 2 | 1 | full | 5 | 0
9 | v15 | 47.15.15.13 | 45.155.155.155 | 47.15.15.15 | 8 | 1 | full | 6 | 0
Entry Index | Port | IP Address | Neighbor Index | Router Id | Options | Priority | State | Events | Retransmission Q Length
Configurations: [Area] [Area Range] [Interface] [Virtual Link] [Trap]
Statistics: [Area] [Interface] [External Link State DB] [Link State DB] [Neighbor]
[ABR ASBR Routers] [Virtual Interface] [Virtual Neighbor]
[Home] [Site Map] [Logout] [Save] [Frame Enable|Disable] [TELNET]

Table 32 describes the fields in the **OSPF Neighbor** window.

TABLE 32 Description of the fields in the **OSPF Neighbor** window

Field	Description
Entry Index	Displays the row number of the entry in the OSPF Neighbor table.
Port	Displays the port through which the Layer 3 switch is connected to the neighbor. This is the port on which an OSPF point-to-point link is configured.
IP Address	Displays the IP address of this Layer 3 switch interface with the neighbor.

TABLE 32 Description of the fields in the **OSPF Neighbor** window (Continued)

Field	Description
Neighbor Index	Displays the IP address of the neighbor. For point-to-point links, the value is as follows: • If the **Priority** field is **1**, this value is the IP address of the neighbor router interface. • If the **Priority** field is **3**, this is the subnet IP address of the neighbor router interface.
Router Id	Displays the neighbor router IP address.
Options	Displays the sum of the option bits in the Options field of the Hello packet.
Priority	Displays the OSPF priority of the neighbor: • For point-to-point links, this field shows one of the following values: – **1** = Point-to-point link – **3** = Point-to-point link with assigned subnet • For multi-access networks, the priority is used during election of the DR and BDR.
State	Displays the state of the conversation between the Layer 3 switch and the neighbor, which can be one of the following values: • **Down** – The initial state of a neighbor conversation. This value indicates that there has been no recent information received from the neighbor. • **Full** - The neighboring Layer 3 switches are fully adjacent. These adjacencies will now appear in Layer 3 switch links and network link advertisements. • **Attempt** – This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor. • **Init** – A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. (The Layer 3 switch itself did not appear in the neighbor's Hello packet.) All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface. • **2-Way** – Communication between the two Layer 3 switches is bidirectional. This is the most advanced state before beginning adjacency establishment. The DR and BDR are selected from the set of neighbors in the 2-Way state or greater. • **ExStart** – The first step in creating an adjacency between the two neighboring Layer 3 switches. The goal of this step is to decide which Layer 3 switch is the master, and to decide upon the initial Database Description (DD) sequence number. Neighbor conversations in this state or greater are called adjacencies. • **Exchange** – The Layer 3 switch is describing its entire link state database by sending DD packets to the neighbor. Each Database Description (DD) packet has a DD sequence number, and is explicitly acknowledged. Only one DD packet can be outstanding at any time. In this state, Link State Request packets can also be sent asking for the neighbor's more recent advertisements. All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets. • **Loading** – Link State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state.
Events	The number of times the neighbor state changed.
Retransmission Q Length	Displays the retransmission queue length.

The **OSPF Neighbor** window provides links to configure and monitor OSPF parameters:

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Displaying OSPF virtual interfaces

To display the OSPF virtual interface information, perform the following the steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **Virtual Interface**.

The **OSPF Virtual Interface** window is displayed as shown in Figure 46.

FIGURE 46 Monitoring OSPF virtual interfaces

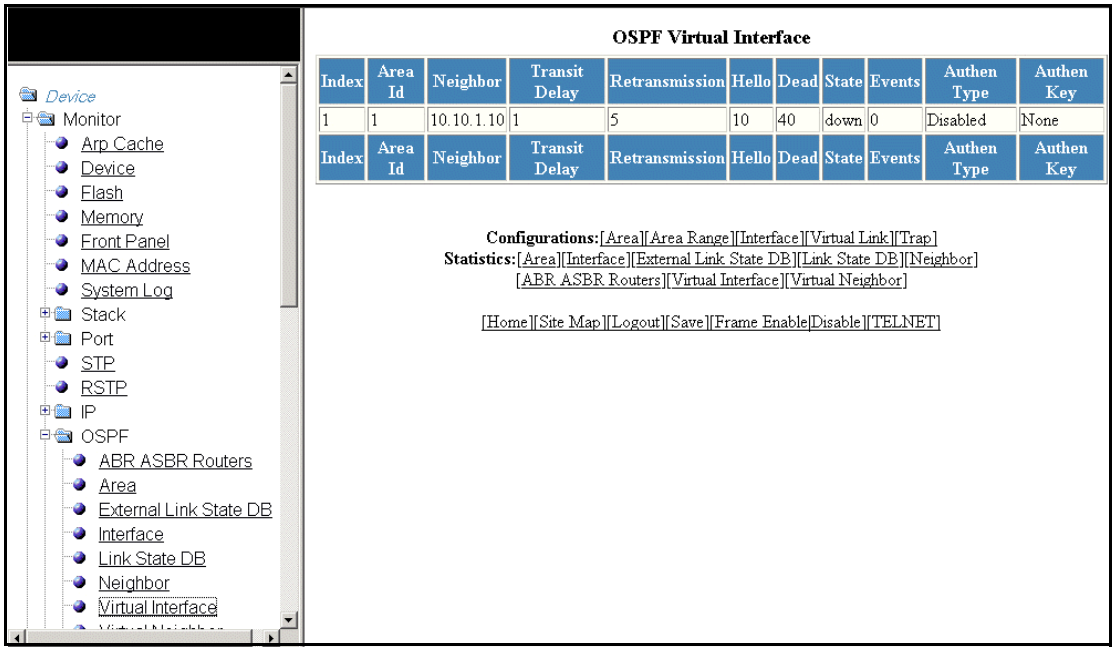


Table 33 describes the fields in the **OSPF Virtual Interface** window.

TABLE 33 Description of the fields in the **OSPF Virtual Interface** window

Field	Description
Index	Displays the row number of the entry in the OSPF Virtual Interface table.
Area Id	Displays the value of the area in which the interface belongs.
Neighbor	Displays the router ID (IP address) of the neighbor.
Transit Delay	Displays the amount of time, in seconds, it takes to transmit Link State Updates packets on the interface.
Retransmission	Displays the number of LSAs retransmitted to adjacent Layer 3 switches for an interface.
Hello	Displays the number of Hello packets transmitted and received by the interface. Also, the total number of bytes associated with transmitted and received Hello packets.
Dead	Displays the number of seconds that a neighbor Layer 3 switch waits for a Hello packet from the current Layer 3 switch before declaring the Layer 3 switch is down.
State	Displays the state of the interface, which can be one of the following: • **DesRouter** – The interface is functioning as the DR for OSPF. • **BackupDesRouter** – The interface is functioning as the BDR for OSPF. • **Loopback** – The interface is functioning as a loopback interface. • **PtToPt** – The interface is functioning as a point-to-point interface. • **Passive** – The interface is up but it does not take part in forming an adjacency. • **Waiting** – The interface is trying to determine the identity of the BDR for the network. • **None** – The interface does not take part in the OSPF interface state machine. • **Down** – The interface is unusable. No protocol traffic can be sent or received on such an interface. • **DesRouter other** – The interface is a broadcast or NBMA network on which another router is selected to be the DR.

TABLE 33 Description of the fields in the **OSPF Virtual Interface** window (Continued)

Field	Description
Events	Displays the OSPF interface event, which can be one of the following: • **0** – Interface Up • **1** – Wait Timer • **2** – Backup Seen • **3** – Neighbor Change • **4** – Loop Indication • **5** – Unloop Indication • **6** – Interface Down • **7** – Interface Passive
Authen Type	Displays whether authentication is enabled on the interface.
Authen Key	Displays the authentication methods for each interface, which can be one of the following: • **None** • **Simple Password** • **MD5**

The **OSPF Virtual Interface** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Displaying OSPF virtual neighbors

To display the OSPF virtual neighbor information, perform the following steps.

1. Click **Monitor** on the left pane and select **OSPF**.
2. Click **Virtual Neighbor**.

The **OSPF Virtual Neighbor** window is displayed as shown in Figure 47.

FIGURE 47 Monitoring OSPF virtual neighbors

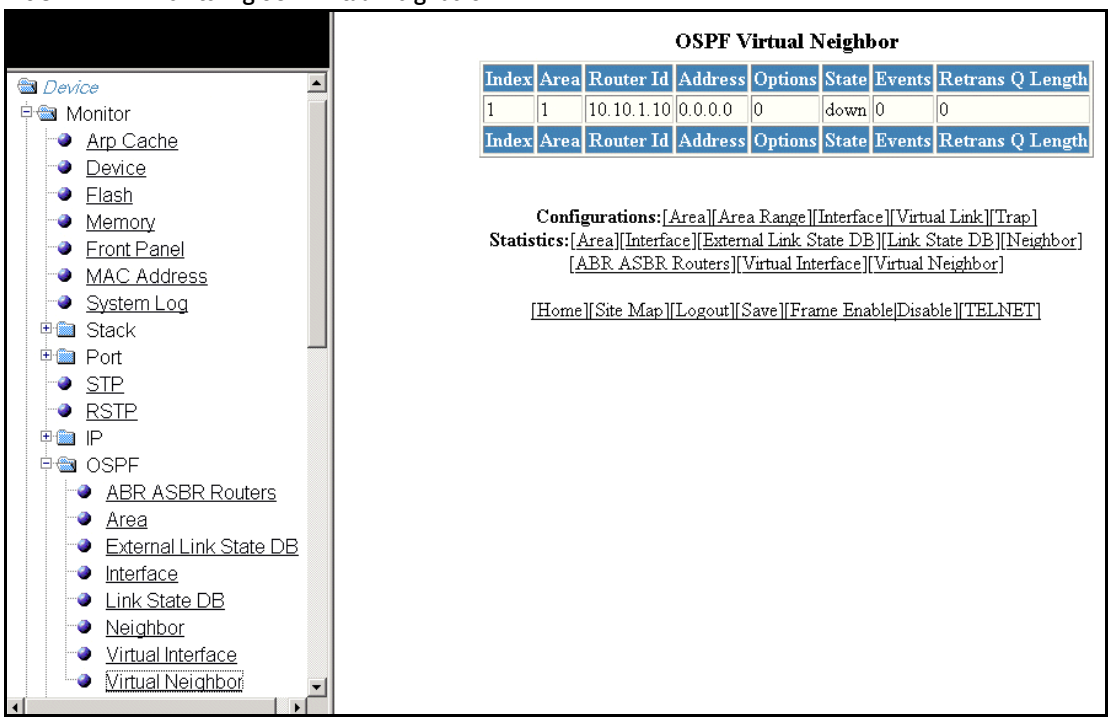


Table 34 describes the fields in the **OSPF Virtual Neighbor** window.

TABLE 34 Description of the fields in the OSPF Virtual Neighbor window

Field	Description
Index	Displays the row number of the entry in the OSPF Virtual Neighbor table.
Area	Displays the area number.
Router Id	Displays the neighbor router IP address.
Address	Displays the OSPF virtual neighbor IP address.
Options	Displays the value of the OSPF header Option field.

TABLE 34 Description of the fields in the **OSPF Virtual Neighbor** window (Continued)

Field	Description
State	Displays the state of the conversation between the Layer 3 switch and the neighbor, which can be one of the following values: • **Down** – The initial state of a neighbor conversation. This value indicates that there has been no recent information received from the neighbor. • **Attempt** – This state is only valid for neighbors attached to non-broadcast networks. It indicates that no recent information has been received from the neighbor. • **Init** – A Hello packet has recently been seen from the neighbor. However, bidirectional communication has not yet been established with the neighbor. (The Layer 3 switch itself did not appear in the neighbor's Hello packet.) All neighbors in this state (or higher) are listed in the Hello packets sent from the associated interface. • **2-Way** – Communication between the two Layer 3 switches is bidirectional. This is the most advanced state before beginning adjacency establishment. The DR and BDR are selected from the set of neighbors in the 2-Way state or greater. • **ExStart** – The first step in creating an adjacency between the two neighboring Layer 3 switches. The goal of this step is to decide which Layer 3 switch is the master, and to decide upon the initial DD sequence number. Neighbor conversations in this state or greater are called adjacencies. • **Exchange** – The Layer 3 switch is describing its entire link state database by sending DD packets to the neighbor. Each DD packet has a DD sequence number, and is explicitly acknowledged. Only one DD packet can be outstanding at any time. In this state, Link State Request packets can also be sent asking for the neighbor's more recent advertisements. All adjacencies in Exchange state or greater are used by the flooding procedure. In fact, these adjacencies are fully capable of transmitting and receiving all types of OSPF routing protocol packets. • **Loading** – Link State Request packets are sent to the neighbor asking for the more recent advertisements that have been discovered (but not yet received) in the Exchange state. • **Full** – The neighboring Layer 3 switches are fully adjacent. These adjacencies will now appear in Layer 3 switch links and network link advertisements.
Events	Displays the number of times the neighbor state changed.
Retrans Q Length	Displays the retransmission queue length.

The **OSPF Virtual Neighbor** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.

- To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
- To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
- To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
- To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
- To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
- To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
- To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

Chapter

9

Monitoring PIM

In this chapter

- Displaying the PIM neighbors 89
- Displaying the PIM virtual interface 90

NOTE
The Protocol Independent Multicast (PIM) feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

Displaying the PIM neighbors

To display information of the Layer 3 switch PIM neighbors, perform the following steps.

1. Click **Monitor** on the left pane and select **PIM**.
2. Click **Neighbor**.

The **PIM Neighbor** window is displayed as shown in Figure 48.

FIGURE 48 Monitoring the PIM neighbors

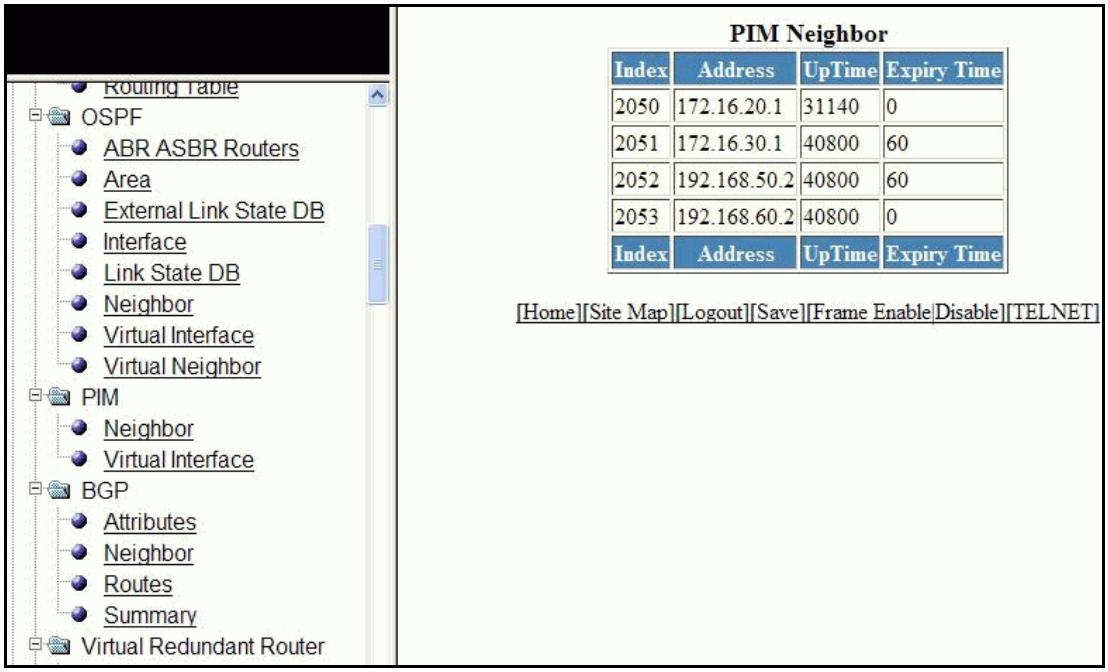


Table 35 describes the fields in the **PIM Neighbor** window.

TABLE 35 Description of the fields in the **PIM Neighbor** window

Field	Description
Index	Displays the row number of the entry in the PIM Neighbor table.
Address	Displays the IP address of the PIM neighbor interface.
UpTime	Displays the number of seconds the PIM neighbor has been up. This timer starts when the Layer 3 switch receives the first Hello packets from the neighbor.
Expiry Time	Displays the amount of time remaining before the route is considered valid in the absence of the next route update.

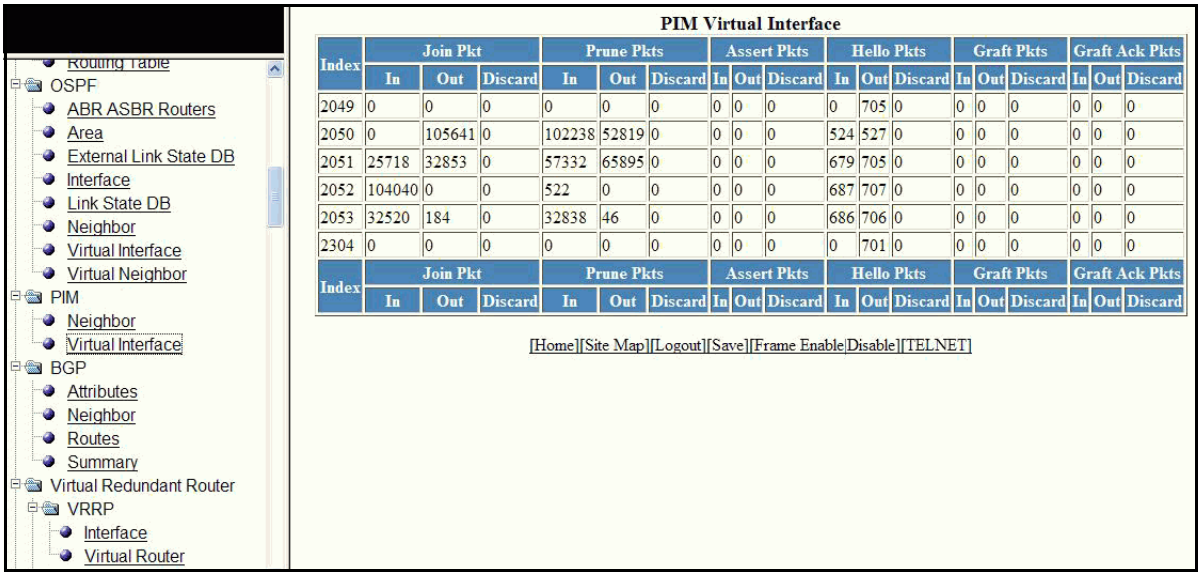
Displaying the PIM virtual interface

To display information of the PIM virtual interfaces, perform the following steps.

1. Click **Monitor** on the left pane and select **PIM**.
2. Click **Virtual Interface**.

The **PIM Virtual Interface** window is displayed as shown in Figure 49.

FIGURE 49 Monitoring the PIM virtual interface



Index	Join Pkt			Prune Pkts			Assert Pkts			Hello Pkts			Graft Pkts			Graft Ack Pkts		
	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard
2049	0	0	0	0	0	0	0	0	0	0	705	0	0	0	0	0	0	0
2050	0	105641	0	102238	52819	0	0	0	0	524	527	0	0	0	0	0	0	0
2051	25718	32853	0	57332	65895	0	0	0	0	679	705	0	0	0	0	0	0	0
2052	104040	0	0	522	0	0	0	0	0	687	707	0	0	0	0	0	0	0
2053	32520	184	0	32838	46	0	0	0	0	686	706	0	0	0	0	0	0	0
2304	0	0	0	0	0	0	0	0	0	0	701	0	0	0	0	0	0	0
Index	Join Pkt			Prune Pkts			Assert Pkts			Hello Pkts			Graft Pkts			Graft Ack Pkts		
	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard

Table 36 describes the fields in the **PIM Virtual Interface** window.

TABLE 36 Description of the fields in the **PIM Virtual Interface** window

Field	Description
Index	Displays the row number of the entry in the PIM Virtual Interface table.
Join Pkt	Displays the following information: • **In** – The number of Join messages received on the interface. • **Out** – The number of Join messages sent by the interface. • **Discard** – The number of Join messages discarded.
Prune Pkts	Displays the following information: • **In** – The number of Prune messages received on the interface • **Out** – The number of Prune messages sent by the interface. • **Discard** – The number of Prune messages discarded.
Assert Pkts	Displays the following information: • **In** – The number of Assert messages received on the interface. • **Out** – The number of Assert messages sent by the interface. • **Discard** – The number of Assert messages discarded.
Hello Pkts	Displays the following information: • **In** – The number of PIM Hello messages received on the interface. • **Out** – The number of PIM Hello messages sent by the interface. • **Discard** – The number of Hello messages discarded.
Graft Pkts	Displays the following information: • **In** – The number of Graft packets received by the upstream Layer 3 switch. • **Out** – The number of Graft packets sent by the downstream Layer 3 switch. • **Discard** – The number of Graft packets discarded.
Graft Ack Pkts	Displays the following information: • **In** – The number of Graft acknowledgment packets received by the downstream Layer 3 switch. • **Out** – The number of Graft acknowledgment packets sent by the upstream Layer 3 switch. • **Discard** – The number of Graft acknowledge packets discarded.

Chapter

Monitoring DVMRP

10

In this chapter

- Displaying DVMRP neighbors 93
- Displaying DVMRP next hop entries 94
- Displaying DVMRP routes 95
- Displaying DVMRP virtual interfaces 96

NOTE
The Distance Vector Multicast Routing Protocol (DVMRP) feature is specific to Brocade FSX devices running Layer 3 code. Brocade FCX and Brocade ICX 6610 devices do not support DVMRP.

Displaying DVMRP neighbors

To display the DVMRP neighbors information, perform the following steps.

1. Click **Monitor** on the left pane and select **DVMRP**.
2. Click **Neighbor**.

The **DVMRP Neighbor** window is displayed as shown in Figure 50.

FIGURE 50 Monitoring DVMRP neighbors

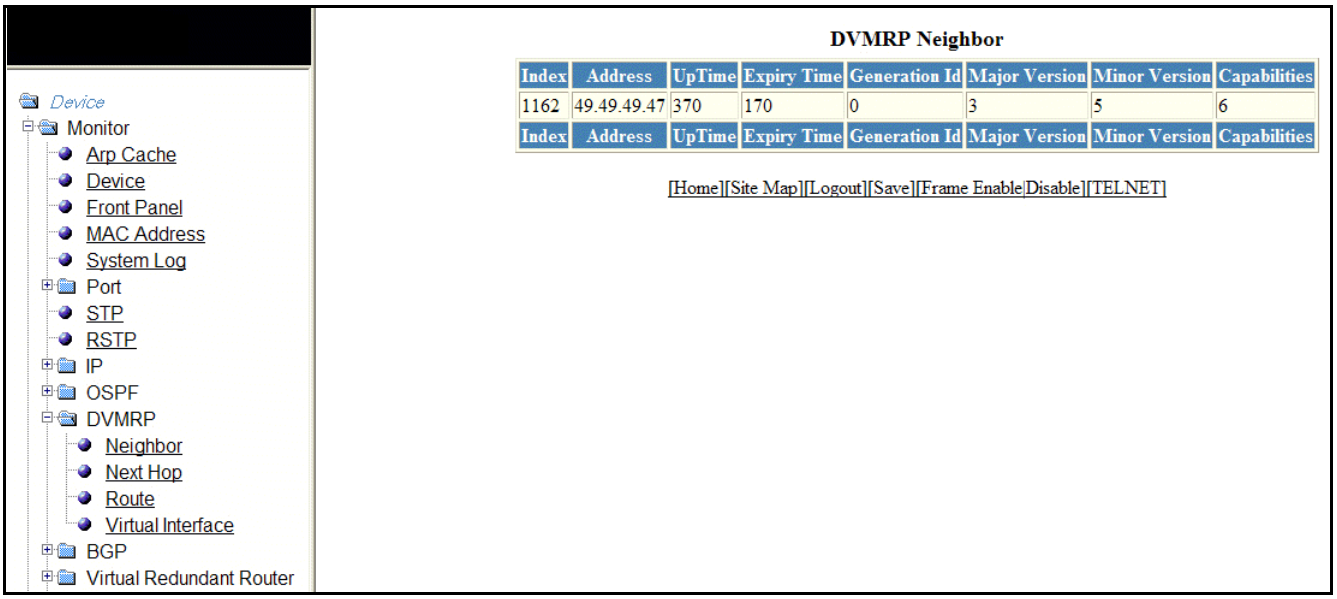


Table 37 describes the fields in the **DVMRP Neighbor** window.

TABLE 37 Description of the fields in the **DVMRP Neighbor** window

Field	Description
Index	Displays the row number of the entry in the DVMRP Neighbor table.
Address	Displays the IP address of the neighbor.
UpTime	Displays the number of seconds the DVMRP neighbor has been up.
Expiry Time	Displays the amount of time remaining before the route is considered valid in the absence of the next route update.
Generation Id	Displays the number that the neighbor generates every time the DVMRP Layer 3 switch restarts.
Major Version	Displays the major version number of the DVMRP on the neighbor.
Minor Version	Displays the minor version number of the DVMRP on the neighbor.
Capabilities	Displays the role that the neighbor is capable of in a network.

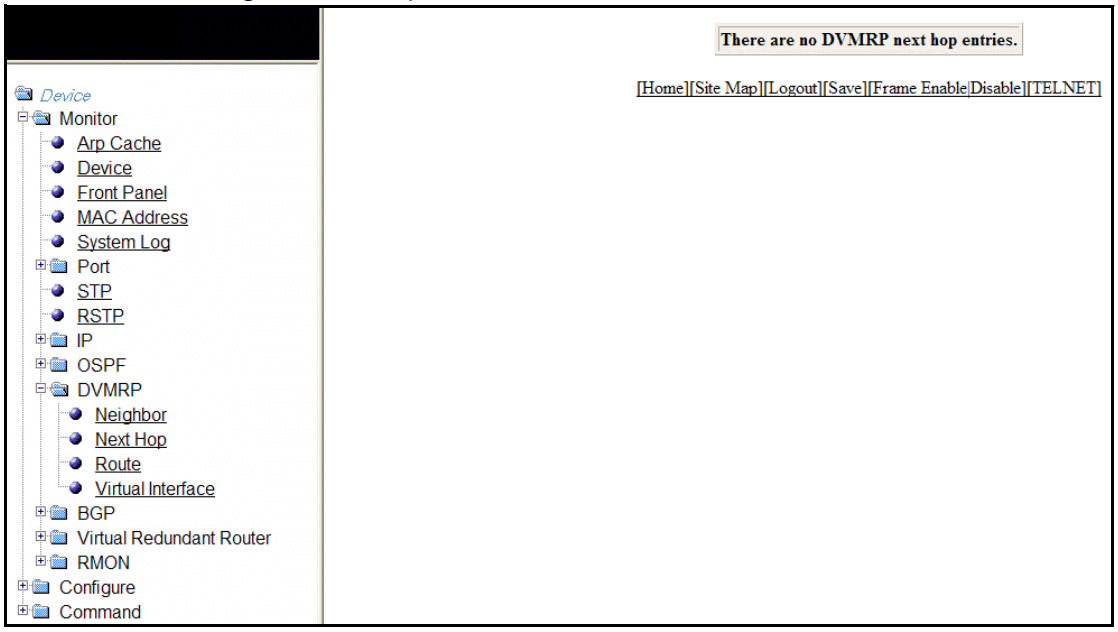
Displaying DVMRP next hop entries

To display the DVMRP next hop information, perform the following steps.

1. Click **Monitor** on the left pane and select **DVMRP**.
2. Click **Next Hop**.

The **DVMRP Next Hop** window is displayed as shown in Figure 51.

FIGURE 51 Monitoring DVMRP next hops



Displaying DVMRP routes

To display the DVMRP route information, perform the following steps.

1. Click **Monitor** on the left pane and select **DVMRP**.
2. Click **Route**.

The **DVMRP Route** window is displayed as shown in Figure 52.

FIGURE 52 Monitoring DVMRP routes

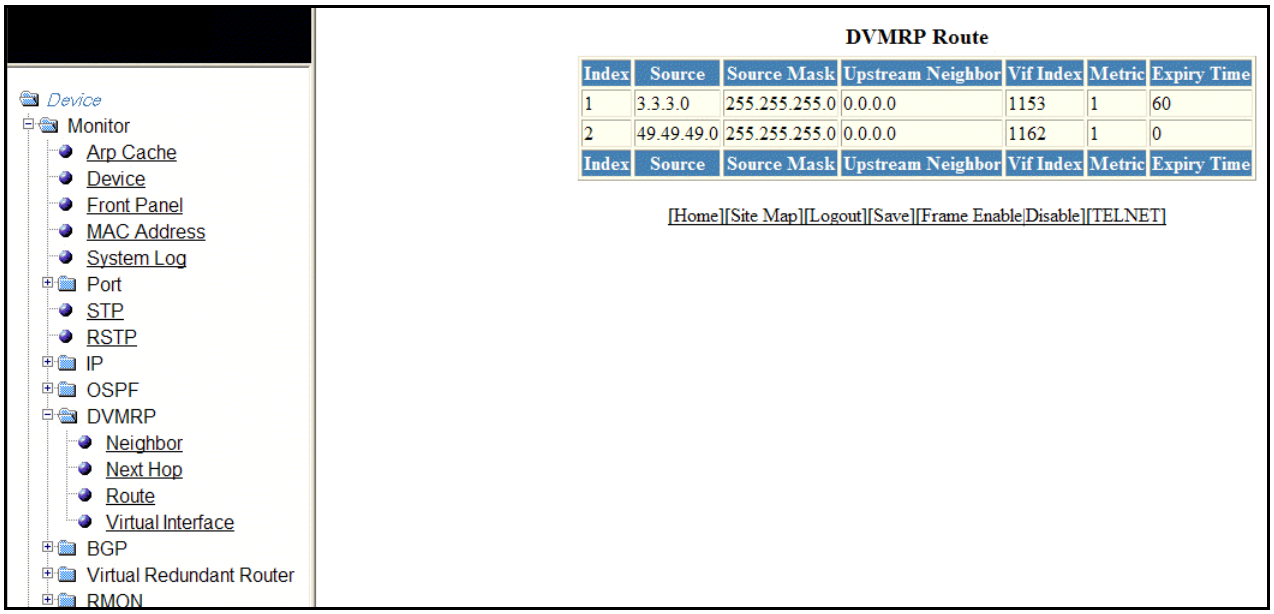


Table 38 describes the fields in the **DVMRP Route** window.

TABLE 38 Description of the fields in the DVMRP Route window

Field	Description
Index	Displays the row number of the entry in the DVMRP Route table.
Source	Displays the source IP address.
Source Mask	Displays the subnet mask for the source IP address.
Upstream Neighbor	Displays the IP address of the upstream neighbor Layer 3 switch.
Vif Index	Displays the entry number of the virtual interface.
Metric	Displays the cost of the upstream neighbor Layer 3 switch.
Expiry Time	Displays how long (in seconds) a route is considered valid in the absence of the next route update.

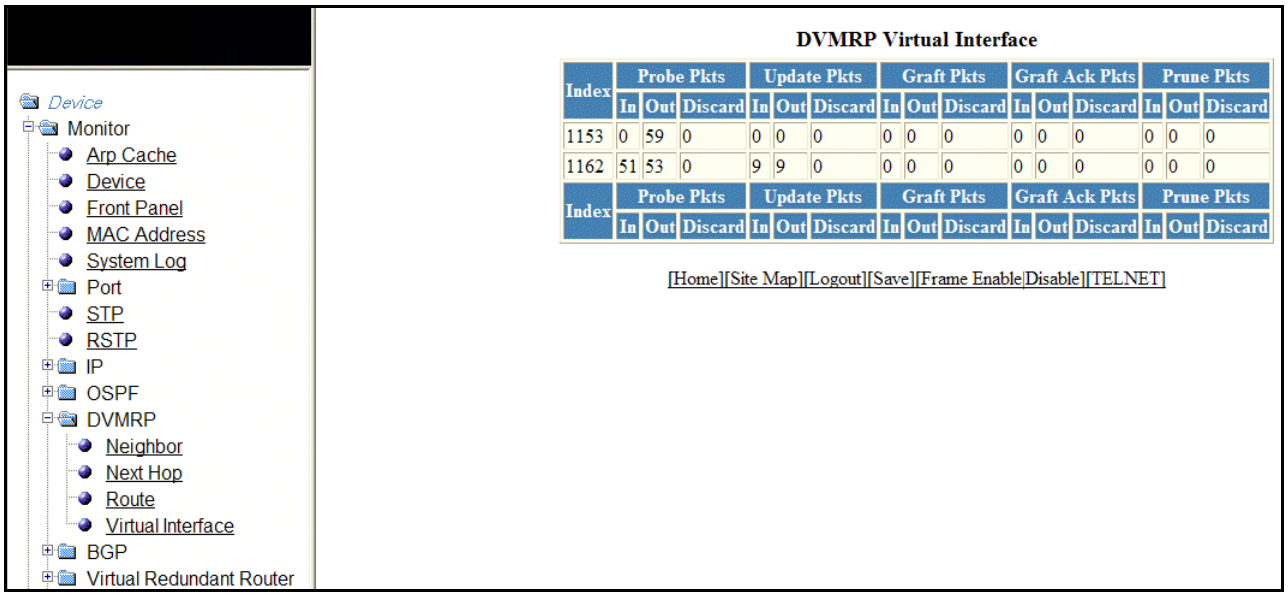
Displaying DVMRP virtual interfaces

To display the DVMRP virtual interface information, perform the following steps.

1. Click **Monitor** on the left pane and select **DVMRP**.
2. Click **Virtual Interface**.

The **DVMRP Virtual Interface** window is displayed as shown in Figure 53.

FIGURE 53 Monitoring DVMRP virtual interfaces



Index	Probe Pkts			Update Pkts			Graft Pkts			Graft Ack Pkts			Prune Pkts		
	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard
1153	0	59	0	0	0	0	0	0	0	0	0	0	0	0	0
1162	51	53	0	9	9	0	0	0	0	0	0	0	0	0	0
Index	Probe Pkts			Update Pkts			Graft Pkts			Graft Ack Pkts			Prune Pkts		
	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard	In	Out	Discard

Table 39 describes the fields in the **DVMRP Virtual Interface** window.

TABLE 39 Description of the fields in the DVMRP Virtual Interface window

Field	Description
Index	Displays the row number of the entry in the DVMRP Virtual Interface table.
Probe Pkts	Displays the following information: • **In** – The number of Probe packets received by a DVMRP neighbor Layer 3 switch. • **Out** – The number of Probe packets sent by the DVMRP Layer 3 switch to the IP multicast group address. • **Discard** – The number of Probe packets discarded.
Update Pkts	Displays the number of routing Update packets sent or received or discarded by DVMRP Layer 3 switches.
Graft Pkts	Displays the following information: • **In** – The number of Graft packets received by the upstream Layer 3 switch. • **Out** – The number of Graft packets sent by the downstream Layer 3 switch. • **Discard** – The number of Graft packets discarded.

TABLE 39 Description of the fields in the **DVMRP Virtual Interface** window (Continued)

Field	Description
Graft Ack Pkts	Displays the following information: • **In** – The number of Graft acknowledgment packets received by the downstream Layer 3 switch. • **Out** – The number of Graft acknowledgment packets sent by the upstream Layer 3 switch. • **Discard** – The number of Graft acknowledgment messages discarded.
Prune Pkts	Displays the following information: • **In** – The number of Prune packets received by the upstream Layer 3 switch. • **Out** – The number of Prune packets sent by the downstream Layer 3 switch. • **Discard** – The number of Prune packets discarded.

Chapter

11

Monitoring BGP

In this chapter

- Displaying BGP attributes 99
- Displaying BGP neighbors 100
- Displaying BGP route statistics 102
- Displaying the BGP neighbor summary 104

NOTE
The Border Gateway Protocol (BGP) feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

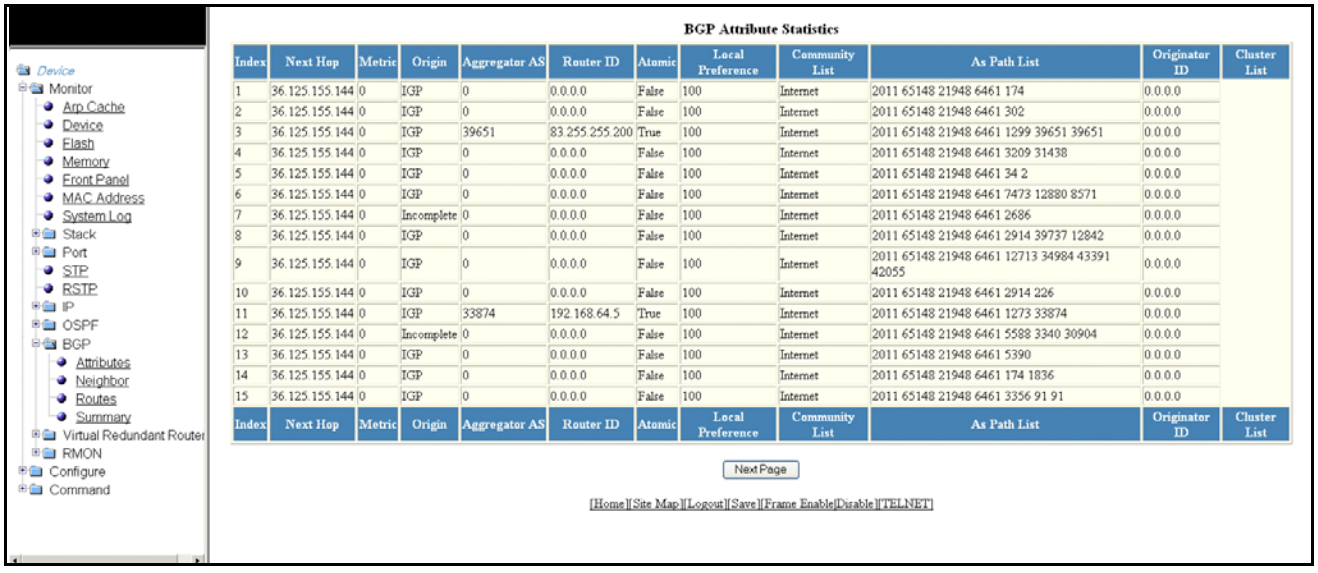
Displaying BGP attributes

To display the BGP attributes information stored in the Layer 3 switch memory, perform the following steps.

1. Click **Monitor** on the left pane and select **BGP**.
2. Click **Attributes**.

The **BGP Attribute Statistics** window is displayed as shown in Figure 54.

FIGURE 54 Monitoring BGP attribute statistics



Index	Next Hop	Metric	Origin	Aggregator AS	Router ID	Atomic	Local Preference	Community List	As Path List	Originator ID	Cluster List
1	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 174	0.0.0.0	
2	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 302	0.0.0.0	
3	36.125.155.144	0	IGP	39651	83.255.255.200	True	100	Internet	2011 65148 21948 6461 1299 39651 39651	0.0.0.0	
4	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 3209 31438	0.0.0.0	
5	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 34 2	0.0.0.0	
6	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 7473 12880 8571	0.0.0.0	
7	36.125.155.144	0	Incomplete	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 2686	0.0.0.0	
8	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 2914 39737 12842	0.0.0.0	
9	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 12713 34984 43391 42055	0.0.0.0	
10	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 2914 226	0.0.0.0	
11	36.125.155.144	0	IGP	33874	192.168.64.5	True	100	Internet	2011 65148 21948 6461 1273 33874	0.0.0.0	
12	36.125.155.144	0	Incomplete	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 5588 3340 30904	0.0.0.0	
13	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 5390	0.0.0.0	
14	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 174 1836	0.0.0.0	
15	36.125.155.144	0	IGP	0	0.0.0.0	False	100	Internet	2011 65148 21948 6461 3356 91 91	0.0.0.0	
Index	Next Hop	Metric	Origin	Aggregator AS	Router ID	Atomic	Local Preference	Community List	As Path List	Originator ID	Cluster List

Table 40 describes the fields in the **BGP Attribute Statistics** window.

TABLE 40 Description of the fields in the **BGP Attribute Statistics** window

Field	Description
Index	Displays the row number of the entry in the BGP Attribute Statistics table.
Next Hop	Displays the IP address of the next hop Layer 3 switch for routes that have this set of attributes.
Metric	Displays the cost of the routes that have this set of attributes.
Origin	Displays the source of the route information, which can be one of the following: • **EGP** – The routes with this set of attributes came to Border Gateway Protocol (BGP) through Exterior Gateway Protocol (EGP). • **IGP** – The routes with this set of attributes came to BGP through IGP. • **INCOMPLETE** – The routes came from an origin other than EGP and IGP. For example, they may have been redistributed from OSPF or RIP.
Aggregator AS	Displays the Autonomous System (AS) in which the network information in the attribute set was aggregated. This value applies only to aggregated routes and is otherwise 0.
Router ID	Displays the IP address of the Layer 3 switch that originated this aggregator.
Atomic	Shows whether the network information in this set of attributes has been aggregated and this aggregation has resulted in information loss: • **TRUE** – Indicates information loss has occurred. • **FALSE** – Indicates no information loss has occurred. **NOTE:** Information loss under these circumstances is a normal part of BGP and does not indicate an error.
Local Preference	Displays the degree of preference for routes that use this set of attributes relative to other routes in the local AS.
Community List	Displays the communities that routes with this set of attributes.
As Path List	Displays the ASes through which routes with this set of attributes have passed.
Originator ID	Displays the originator of the route in a route reflector environment.
Cluster List	Displays the route-reflector clusters through which this set of attributes has passed.

To display the next set of BGP attributes, click **Next Page**.

Displaying BGP neighbors

To display BGP neighbor information, perform the following steps.

1. Click **Monitor** on the left pane and select **BGP**.
2. Click **Neighbor**.

The **BGP Neighbor Statistics** window is displayed as shown in Figure 55.

FIGURE 55 Monitoring BGP neighbor statistics

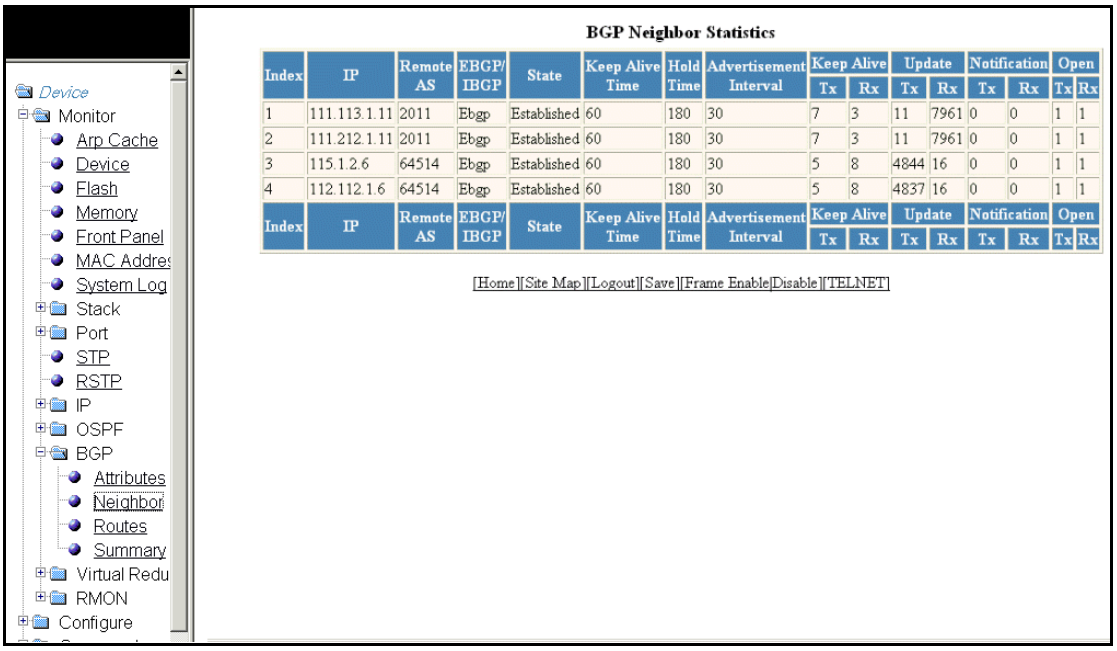

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Addres
System Log
Stack
Port
STP
RSTP
IP
OSPF
BGP
Attributes
Neighbor
Routes
Summary
Virtual Redu
RMON
Configure
BGP Neighbor Statistics
Index IP Remote AS EBGP/IBGP State Keep Alive Time Hold Time Advertisement Interval Keep Alive Update Notification Open
Tx Rx Tx Rx Tx Rx Tx Rx
1 111.113.1.11 2011 Ebgp Established 60 180 30 7 3 11 7961 0 0 1 1
2 111.212.1.11 2011 Ebgp Established 60 180 30 7 3 11 7961 0 0 1 1
3 115.1.2.6 64514 Ebgp Established 60 180 30 5 8 4844 16 0 0 1 1
4 112.112.1.6 64514 Ebgp Established 60 180 30 5 8 4837 16 0 0 1 1
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 41 describes the fields in the **BGP Neighbor Statistics** window.

TABLE 41 Description of the fields in the **BGP Neighbor Statistics** window

Field	Description
Index	Displays the row number of the entry in the BGP Neighbors Statistics table.
IP	Displays the IP address of the neighbor.
Remote AS	Displays the AS the neighbor is in.
EBGP/IBGP	Indicates whether the neighbor session is an Interior Border Gateway Protocol (IBGP) session or an Exterior Border Gateway Protocol (EBGP) session: • **IBGP** – The neighbor is in the same AS. • **EBGP** – The neighbor is in another AS.
State	Displays the state of the Layer 3 switch session with the neighbor. The states are from this Layer 3 switch perspective of the session, not the neighbor perspective. Possible states are as follows: • **Established** – The BGP is ready to exchange UPDATE messages with the neighbor. • **Idle** – The BGP process is waiting to be started. • **Admnd** – The neighbor has been administratively shut down. • **Connect** – BGP is waiting for the connection process for the TCP neighbor session to be completed. • **Active** – BGP is waiting for a TCP connection from the neighbor. • **Open Sent** – BGP is waiting for an OPEN message from the neighbor. • **Open Confirm** – BGP has received an OPEN message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the Layer 3 switch receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle.
Keep Alive Time	Displays the keep alive time, which specifies how often this Layer 3 switch sends KEEPALIVE messages to the neighbor.

TABLE 41 Description of the fields in the **BGP Neighbor Statistics** window (Continued)

Field	Description
Hold Time	Displays the hold time, which specifies how many seconds the Layer 3 switch waits for a KEEPALIVE or UPDATE message from a BGP neighbor before deciding that the neighbor is dead.
Advertisement Interval	Displays the minimum delay (seconds) between messages to the specified neighbor.
Keep Alive	Displays the following information: • **Tx** – Displays the number of times the Layer 3 switch sends KEEPALIVE messages to its BGP neighbors. • **Rx** – Displays the number of times the Layer 3 switch receives KEEPALIVE messages from its BGP neighbors.
Update	Displays the following information: • **Tx** – Displays the number of times the Layer 3 switch sends BGP route advertisements to its neighbors. • **Rx** – Displays the number of times the Layer 3 switch receives BGP route advertisements from its neighbors.
Notification	Displays the following information: • **Tx** – Displays the number of times the Layer 3 switch sends the NOTIFICATION message to its neighbors. • **Rx** – Displays the number of times the Layer 3 switch receives the NOTIFICATION message from its neighbors.
Open	Displays the following information: • **Tx** – Displays the number of times the Layer 3 switch sends the OPEN message to its neighbors. • **Rx** – Displays the number of times the Layer 3 switch receives the OPEN message from its neighbors.

Displaying BGP route statistics

To display the BGP route information, perform the following steps.

1. Click **Monitor** on the left pane and select **BGP**.
2. Click **Routes**.

The **BGP Route Statistics** window is displayed as shown in Figure 56.

FIGURE 56 Monitoring BGP route statistics

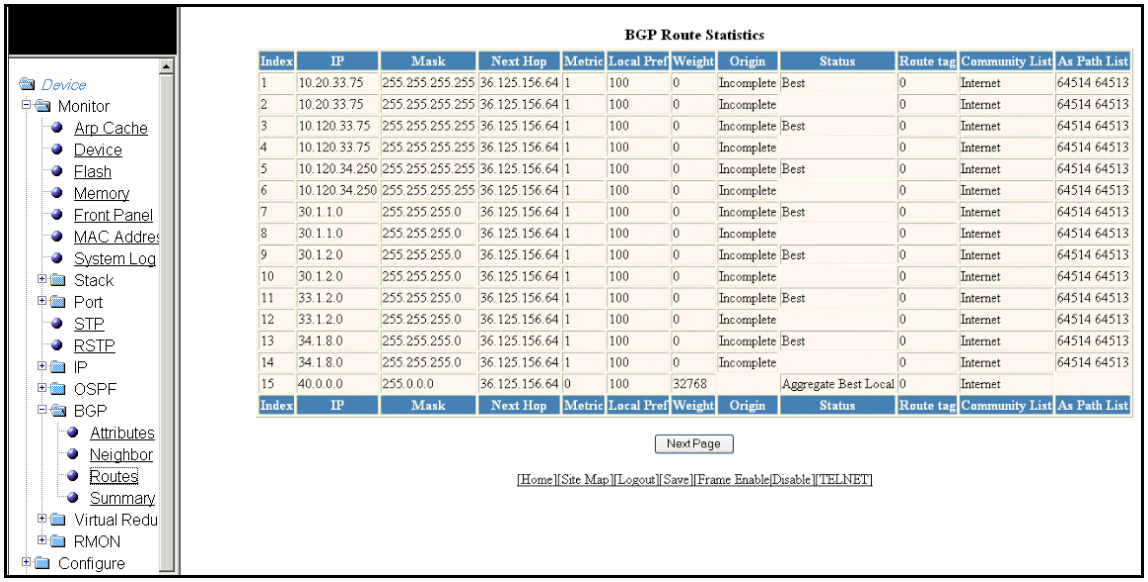

Device
Monitor
Arp Cache
Device
Flash
Memory
Front Panel
MAC Addres
System Log
Stack
Port
STP
RSTP
IP
OSPF
BGP
Attributes
Neighbor
Routes
Summary
Virtual Redu
RMON
Configure
BGP Route Statistics
Index IP Mask Next Hop Metric Local Pref Weight Origin Status Route tag Community List As Path List
1 10.20.33.75 255.255.255.255 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
2 10.20.33.75 255.255.255.255 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
3 10.120.33.75 255.255.255.255 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
4 10.120.33.75 255.255.255.255 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
5 10.120.34.250 255.255.255.255 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
6 10.120.34.250 255.255.255.255 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
7 30.1.1.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
8 30.1.1.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
9 30.1.2.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
10 30.1.2.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
11 33.1.2.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
12 33.1.2.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
13 34.1.8.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete Best 0 Internet 64514 64513
14 34.1.8.0 255.255.255.0 36.125.156.64 1 100 0 Incomplete 0 Internet 64514 64513
15 40.0.0.0 255.0.0.0 36.125.156.64 0 100 32768 Aggregate Best Local 0 Internet
Index IP Mask Next Hop Metric Local Pref Weight Origin Status Route tag Community List As Path List
Next Page
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 42 describes the fields in the **BGP Route Statistics** window.

TABLE 42 Description of the fields in the **BGP Route Statistics** window

Field	Description
Index	Displays the row number of the entry in the BGP Route Statistics table.
IP	Displays the source IP address.
Mask	Displays the subnet mask for the source IP address.
Next Hop	Displays the IP address of the next hop Layer 3 switch for reaching the network from the Layer 3 switch.
Metric	Displays the route metric. If the route does not have a metric, this field displays 0.
Local Pref	Displays the degree of preference for this route relative to other routes in the local AS.
Weight	Displays the value that this Layer 3 switch associates with routes from a specific neighbor.
Origin	Displays the source of the route information, which can be one of the following: • **EGP** – Indicates that the routes with this set of attributes came to BGP through EGP. • **IGP** – Indicates that the routes with this set of attributes came to BGP through IGP. • **Incomplete** – Indicates that the routes came from an origin other than EGP and IGP. For example, they may have been redistributed from OSPF or RIP.

TABLE 42 Description of the fields in the **BGP Route Statistics** window (Continued)

Field	Description
Status	Displays the route status, which can be one or more of the following: • **Best** - BGP has determined that this is the optimal route to the destination. • **Aggregate** - The route is an aggregate route for multiple networks. • **Not-installed-besT** - The routes received from the neighbor are the best BGP routes to their destinations, but were nonetheless not installed in the IP route table because the Layer 3 switch received better routes from other sources (such as OSPF, RIP, or static IP routes). • **Confed_ebgP** - The route was learned from a neighbor in the same confederation and AS, but in a different sub-AS within the confederation. • **Damped** - This route has been dampened (by the route dampening feature), and is currently unusable. • **History** - Route dampening is configured for this route, and the route has a history of flapping and is unreachable now. • **Internal** - The route was learned through BGP. • **Local** - The route originated on this Layer 3 Switch. • **Multipath** - BGP load sharing is enabled and this route was selected as one of the best ones to the destination. • **Suppressed** - This route was suppressed during aggregation and thus is not advertised to neighbors.
Router tag	Displays the Layer 3 switch tag value.
Community List	Displays the communities the route is in.
As Path List	Displays the ASes through which a route passes. BGP Layer 3 switches can use the AS-path to detect and eliminate routing loops.

To display the next set of BGP routes, click **Next Page**.

Displaying the BGP neighbor summary

To display the BGP neighbor information, perform the following steps.

1. Click **Monitor** on the left pane and select **BGP**.
2. Click **Summary**.

The **BGP Neighbor Summary** window is displayed as shown in Figure 57.

FIGURE 57 Monitoring the BGP neighbor summary

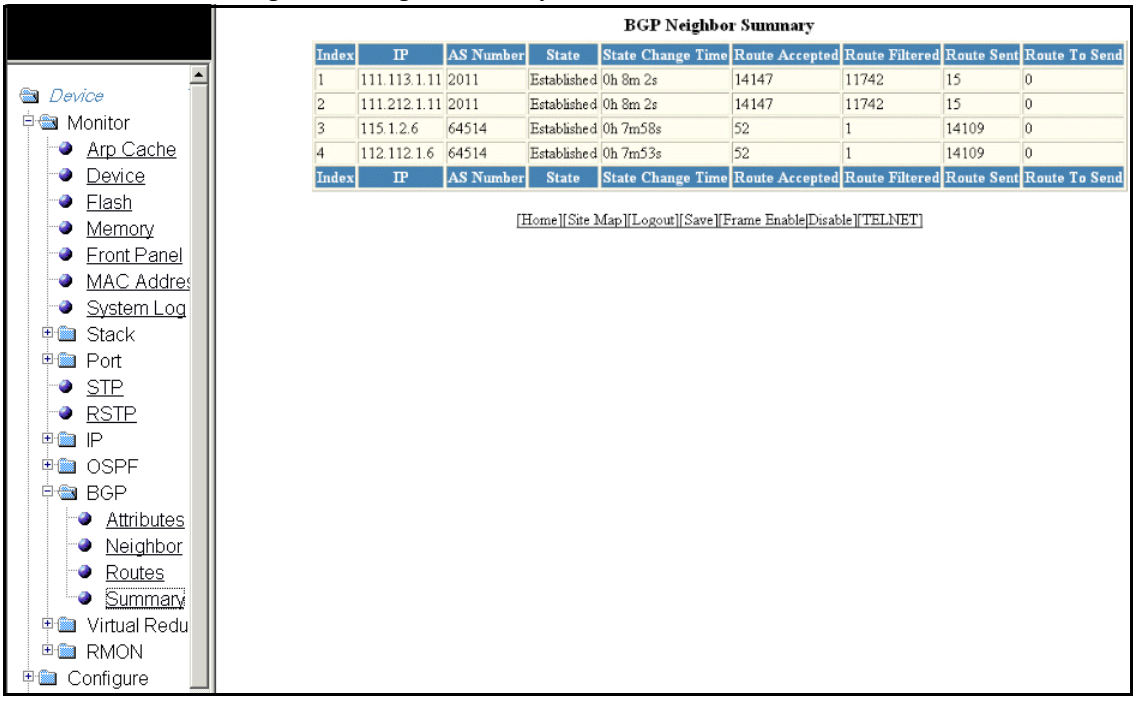


Table 43 describes the fields in the **BGP Neighbor Summary** window.

TABLE 43 Description of the fields in the **BGP Neighbor Summary** window

Field	Description
Index	Displays the row number of the entry in the BGP Neighbor Summary table.
IP	Displays the IP address of the neighbor.
AS Number	Displays the BGP AS number the Layer 3 switch is in.
State	Displays the state of this Layer 3 switch neighbor session with each neighbor. The states are from this Layer 3 switch perspective of the session, not the neighbor perspective. The state values can be one of the following for each Layer 3 switch: • **Established** – The BGP is ready to exchange UPDATE packets with the neighbor. • **Idle** – The BGP4 process is waiting to be started. • **Admnd** – The neighbor has been administratively shut down. • **Connect** –The BGP is waiting for the connection process for the TCP neighbor session to be completed. • **Active** – The BGP is waiting for a TCP connection from the neighbor. • **Open Sent** – The BGP is waiting for an OPEN message from the neighbor. • **Open Confirm** – The BGP has received an OPEN message from the neighbor and is now waiting for either a KEEPALIVE or NOTIFICATION message. If the Layer 3 switch receives a KEEPALIVE message from the neighbor, the state changes to Established. If the message is a NOTIFICATION, the state changes to Idle.
State Change Time	Displays the time that has passed since the state last changed.
Route Accepted	Displays the number of routes received from the neighbor that this Layer 3 switch installed in the BGP route table.

TABLE 43 Description of the fields in the **BGP Neighbor Summary** window (Continued)

Field	Description
Route Filtered	Displays the routes or prefixes that have been filtered out: • If soft reconfiguration is enabled, this field shows how many routes were filtered out (not placed in the BGP route table) but retained in memory. • If soft reconfiguration is not enabled, this field shows the number of BGP routes that have been filtered out.
Route Sent	Displays the number of BGP routes that the Layer 3 switch has sent to the neighbor.
Route To Send	Displays the number of BGP routes the Layer 3 switch has queued to send to this neighbor.

Chapter

Monitoring Virtual Redundant Router 12

In this chapter

- Displaying VRRP interfaces 107
- Displaying VRRP virtual router entries 108
- Displaying VRRP-E interfaces 110
- Displaying VRRP-E virtual router entries 111
- Displaying VSRP virtual switch entries 112

NOTE
The Virtual Redundant Router feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code. In Brocade FSX devices, VRRP is supported in the base Layer 3 software image also.

Displaying VRRP interfaces

To display the Virtual Router Redundancy Protocol (VRRP) interface information, perform the following steps.

1. Click **Monitor** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP** and then select **Interface**.

The **Virtual Router Interface Statistics** window is displayed as shown in Figure 58.

FIGURE 58 Monitoring virtual router interface statistics

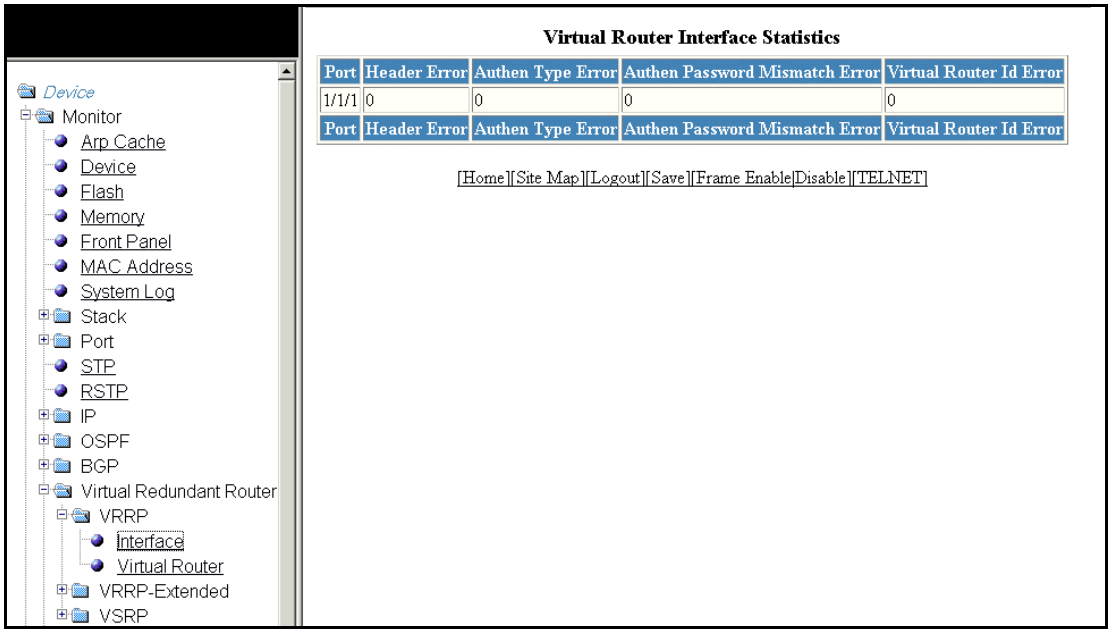


Table 44 describes the fields in the **Virtual Router Interface Statistics** window.

TABLE 44 Description of the fields in the **Virtual Router Interface Statistics** window

Field	Description
Port	Displays the Ethernet port or virtual interface on which VRRP is configured. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Header Error	Displays the number of VRRP packets received by the interface that had a header error.
Authen Type Error	Displays the number of VRRP packets received by the interface that had an authentication error.
Authen Password Mismatch Error	Displays the number of VRRP packets received by the interface that had a password value that does not match the password used by the interface for authentication.
Virtual Router Id Error	Displays the number of VRRP packets received by the interface that contained a Virtual Router ID (VRID) that is not configured on this interface.

Displaying VRRP virtual router entries

To display the VRRP virtual router information, perform the following steps.

1. Click **Monitor** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP** and then select **Virtual Router**.

The **VRRP Virtual Router Statistics** window is displayed as shown in Figure 59.

FIGURE 59 Monitoring VRRP virtual router statistics

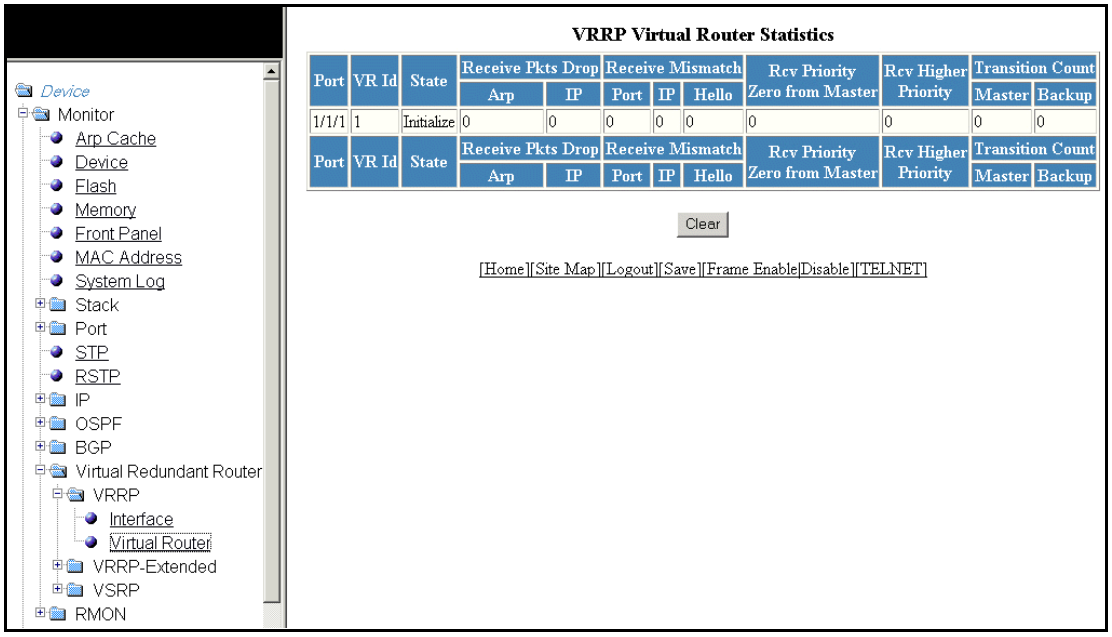


Table 45 describes the fields in the **VRRP Virtual Router Statistics** window.

TABLE 45 Description of the fields in the **VRRP Virtual Router Statistics** window

Field	Description
Port	Displays the Ethernet port or virtual interface on which VRRP is configured. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
VR Id	Displays the VRID configured on an interface.
State	Displays this Layer 3 switch VRRP state for the VRID, which can be one of the following: • **Initialize** – Indicates that the VRID is not enabled (activated). **NOTE:** If the state is "Initialize", the mode is incomplete. Therefore, make sure you have specified the IP address for the VRID. • **Backup** – Indicates that this Layer 3 switch is a Backup for the VRID. • **Master** – Indicates that this Layer 3 switch is the Master for the VRID.
Receive Pkts Drop	Displays the error statistics for the following: • **Arp** – The number of ARP packets addressed to the VRID that were dropped. • **IP** – The number of IP packets addressed to the VRID that were dropped.
Receive Mismatch	Displays the error statistics for the following: • **Port** – The number of packets received that did not match the configuration for the receiving interface. • **IP** – The number of packets received that did not match the configured IP addresses. • **Hello** – The number of packets received that did not match the configured Hello interval.
Rcv Priority Zero from Master	Displays whether the current Master has resigned.

TABLE 45 Description of the fields in the **VRRP Virtual Router Statistics** window (Continued)

Field	Description
Rcv Higher Priority	Displays the number of VRRP packets received by the interface that had a higher backup priority for the VRID than this Layer 3 switch backup priority for the VRID.
Transition Count	Displays the transition count for the following: • **Master** – The number of times this Layer 3 switch has changed from the backup state to the master state for the VRID. • **Backup** – The number of times this Layer 3 switch has changed from the master state to the backup state for the VRID.

To remove the current data in the table and restart monitoring, click **Clear**.

Displaying VRRP-E interfaces

To display the Virtual Router Redundancy Protocol Extended (VRRP-E) interface information, perform the following steps.

1. Click **Monitor** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP-Extended** and then select **Interface**.

The **Virtual Router Interface Statistics** window is displayed as shown in Figure 60.

FIGURE 60 Monitoring virtual router interface statistics

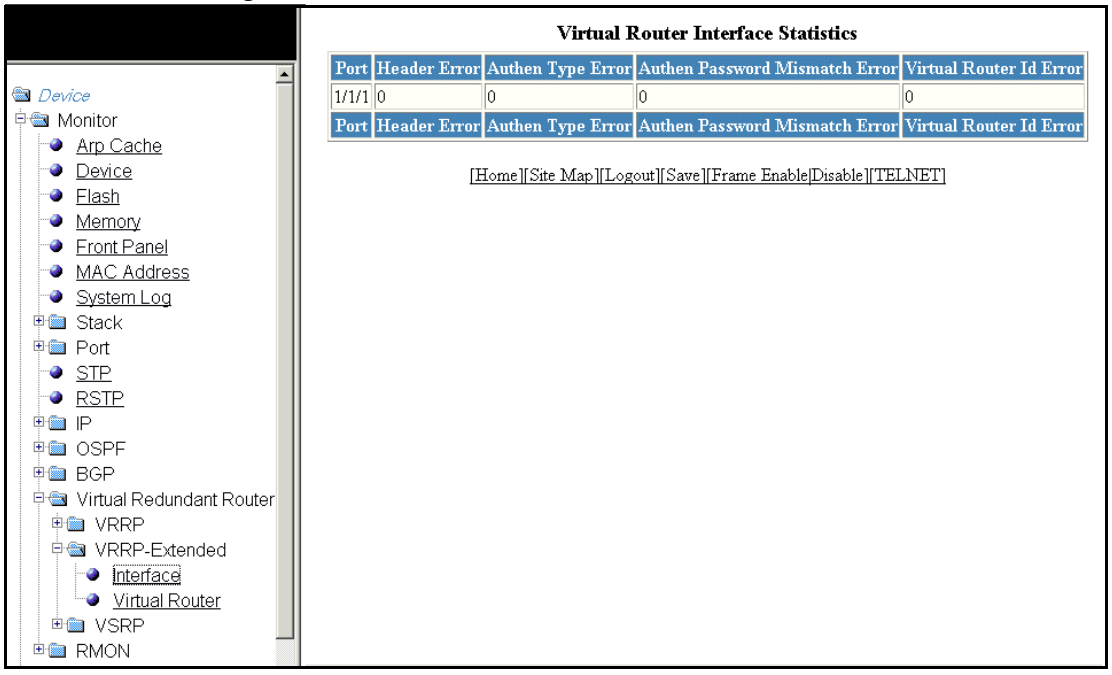


Table 46 describes the fields in the **Virtual Router Interface Statistics** window.

TABLE 46 Description of the fields in the **Virtual Router Interface Statistics** window

Field	Description
Port	Displays the Ethernet port or virtual interface on which VRRP-E is configured. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Header Error	Displays the number of VRRP-E packets received by the interface that had a header error.
Authen Type Error	Displays the number of VRRP-E packets received by the interface that had an authentication error.
Authen Password Mismatch Error	Displays the number of VRRP-E packets received by the interface that had a password value that does not match the password used by the interface for authentication.
Virtual Router Id Error	Displays the number of VRRP-E packets received by the interface that contained a VRID that is not configured on this interface.

Displaying VRRP-E virtual router entries

To display the VRRP-E virtual router information, perform the following steps.

1. Click **Monitor** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP-Extended** and then select **Virtual Router**.

The **VRRP-E Virtual Router Statistics** window is displayed as shown in Figure 61.

FIGURE 61 Monitoring VRRP-E virtual router statistics

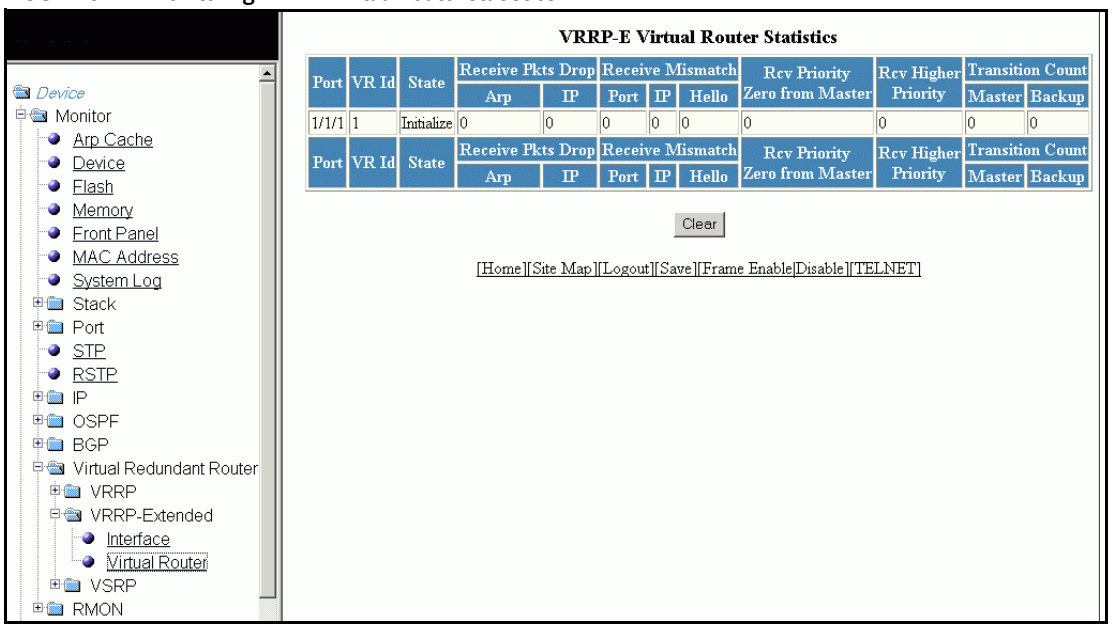


Table 47 describes the fields in the **VRRP-E Virtual Router Statistics** window.

TABLE 47 Description of the fields in the **VRRP-E Virtual Router Statistics** window

Field	Description
Port	Displays the Ethernet port or virtual interface on which VRRP-E is configured. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
VR Id	Displays the VRID configured on an interface.
State	Displays this Layer 3 switch VRRP-E state for the VRID, which can be one of the following: • **Initialize** – Indicates that the VRID is not enabled (activated). **NOTE:** If the state is "Initialize", the mode is incomplete. Therefore, make sure you have specified the IP address for the VRID. • **Backup** – Indicates that this Layer 3 switch is a Backup for the VRID. • **Master** – This Layer 3 switch is the Master for the VRID.
Receive Pkts Drop	Displays the error statistics for the following: • **Arp** – The number of ARP packets addressed to the VRID that were dropped. • **IP** – The number of IP packets addressed to the VRID that were dropped.
Receive Mismatch	Displays the error statistics for the following: • **Port** – The number of packets received that did not match the configuration for the receiving interface. • **IP** – The number of packets received that did not match the configured IP addresses. • **Hello** – The number of packets received that did not match the configured Hello interval.
Rcv Priority Zero from Master	Displays whether the current Master has resigned.
Rcv Higher Priority	Displays the number of VRRP-E packets received by the interface that had a higher backup priority for the VRID than this Layer 3 switch backup priority for the VRID.
Transition Count	Displays the transition count for the following: • **Master** – The number of times this Layer 3 switch has changed from the backup state to the master state for the VRID. • **Backup** – The number of times this Layer 3 switch has changed from the master state to the backup state for the VRID.

Displaying VSRP virtual switch entries

To display the Virtual Switch Redundancy Protocol (VSRP) information, perform the following steps.

1. Click **Monitor** on the left pane and select **Virtual Redundant Router**.
2. Click **VSRP** and then select **Virtual Switch**.

The **VSRP Virtual Switch Statistics** window is displayed as shown in Figure 62.

FIGURE 62 Monitoring VSRP virtual switch statistics

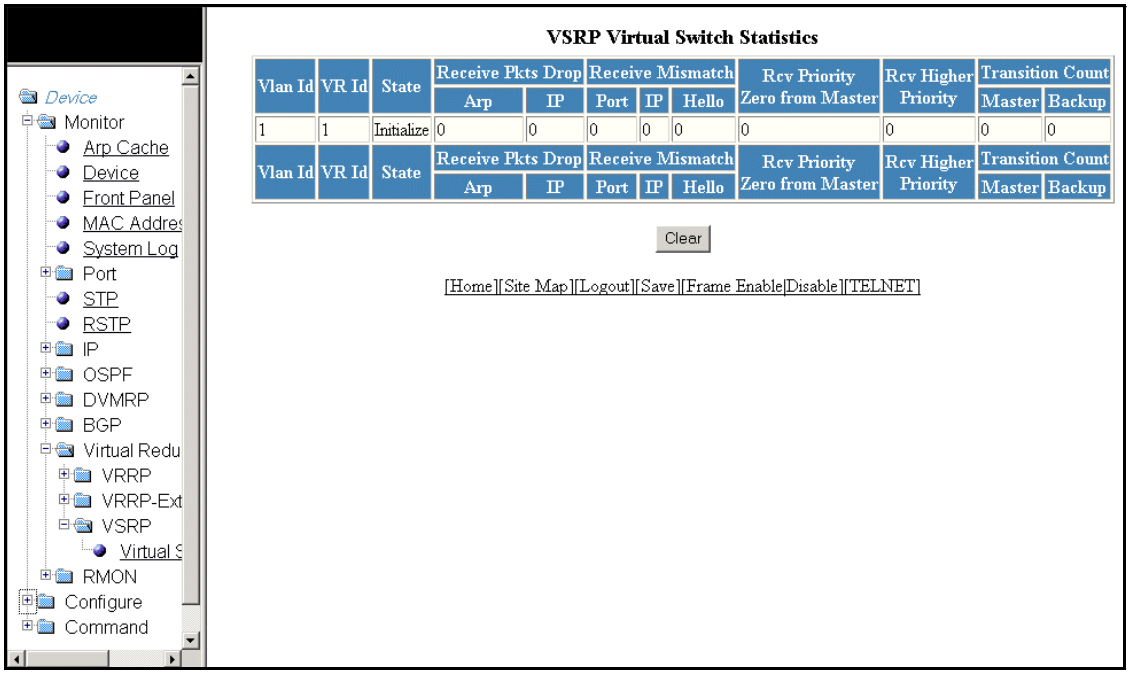


Table 48 describes the fields in the **VSRP Virtual Switch Statistics** window.

TABLE 48 Description of the fields in the **VSRP Virtual Switch Statistics** window

Field	Description
Vlan Id	Displays the VLAN ID on which VSRP is configured.
VR Id	Displays the VRID configured on the interface.
State	Displays this device VSRP state for the VRID, which can be one of the following: • **Initialize** – The VRID is not enabled (activated). **NOTE:** If the state is "Initialize", the mode is incomplete. Therefore, make sure you have specified the IP address for the VRID. • **Standby** – This device is a Backup for the VRID. • **Master** – This device is the Master for the VRID.
Receive Pkts Drop	Displays the error statistics for the following: • **Arp** – The number of ARP packets addressed to the VRID that were dropped. • **IP** – The number of IP packets addressed to the VRID that were dropped.
Receive Mismatch	Displays the error statistics for the following: • **Port** – The number of packets received that did not match the configuration for the receiving interface. • **IP** – The number of packets received that did not match the configured IP addresses. • **Hello** – The number of packets received that did not match the configured Hello interval.
Rcv Priority Zero from Master	Displays whether the current Master has resigned.

TABLE 48 Description of the fields in the **VSRP Virtual Switch Statistics** window (Continued)

Field	Description
Rcv Higher Priority	Displays the number of VSRP packets received by the interface that had a higher backup priority for the VRID than this Layer 3 switch backup priority for the VRID.
Transition Count	Displays the transition count for the following: • **Master** – The number of times this Layer 3 switch has changed from the backup state to the master state for the VRID. • **Backup** – The number of times this Layer 3 switch has changed from the master state to the backup state for the VRID.

Chapter

Monitoring RMON

13

In this chapter

- Displaying RMON history 115
- Displaying RMON Ethernet statistics 117
- Changing polling interval 120
- Displaying RMON Ethernet error statistics 120

Displaying RMON history

By default, all active ports generate two history control data entries per active port. An active port is defined as one with a link up. If the link goes down, the two history entries are automatically cleared.

The following history entries are generated for each device:

- A sampling of statistics every 30 seconds
- A sampling of statistics every 30 minutes

To display Remote Monitoring (RMON) history, perform the following steps.

1. Click **Monitor** on the left pane and select **RMON**.
2. Click **History**.

The **RMON Ethernet History** window is displayed as shown in Figure 63.

FIGURE 63 Monitoring the RMON Ethernet history

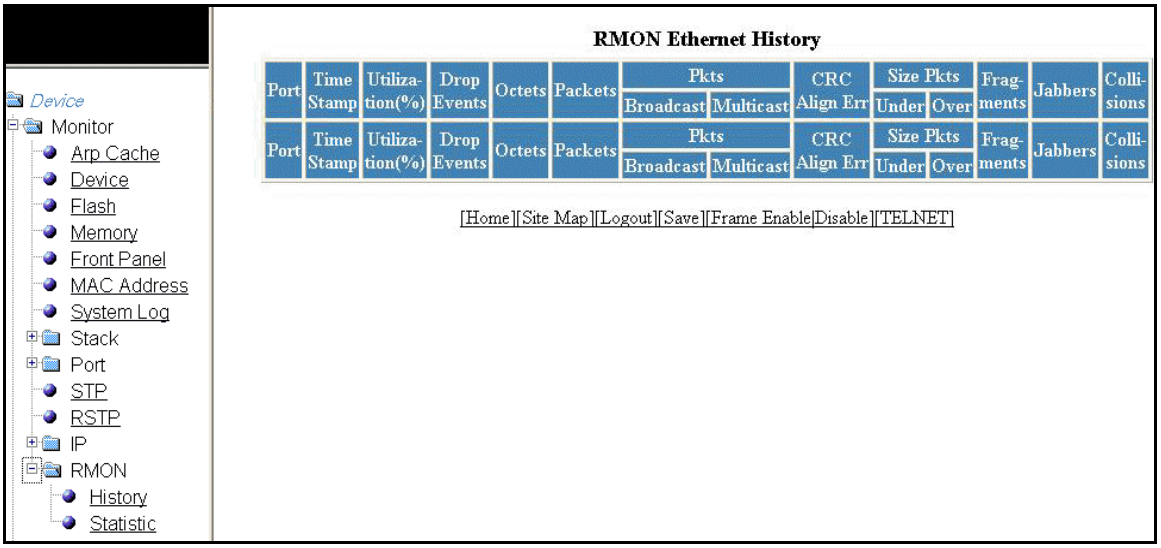


Table 49 describes the fields in the **RMON Ethernet History** window.

TABLE 49 Description of the fields in the **RMON Ethernet History** window

Field	Description
Port	Displays the port for which the history data is being presented. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Time Stamp	Displays the day and time when the data was collected.
Utilization(%)	Displays the percentage of the port that was being utilized when the data was taken.
Drop Events	Displays the total number of events in which packets were dropped by the RMON probe due to lack of resources. This number is not necessarily the number of packets dropped, but is the number of times an overrun condition has been detected.
Octets	Displays the total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.
Packets	Displays the total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.
Packets: Broadcast	Displays the total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Packets: Multicast	Displays the total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
CRC Alignment Errors	Displays the total number of packets received that were from 64 through 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The packet length does not include framing bits but does include FCS octets.
Size Packets: Under	Displays the total number of packets received that were less than 64 octets long and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Size Packets: Over	Displays the total number of packets received that were longer than 1518 octets and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Fragments	Displays the total number of packets received that were less than 64 octets long and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for this counter to be incremented, because it counts both runts (which are normal occurrences due to collisions) and noise hits. This number does not include framing bits but does include FCS octets.

TABLE 49 Description of the fields in the **RMON Ethernet History** window (Continued)

Field	Description
Jabbers	Displays the total number of packets received that were longer than 1518 octets and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **NOTE:** This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. This number does not include framing bits but does include FCS octets.
Collisions	Displays the best estimate of the total number of collisions on this Ethernet segment.

Displaying RMON Ethernet statistics

RMON statistics provide count information on multicast and broadcast packets. This information includes total packets sent, undersized and oversized packets, CRC alignment errors, jabbers, collisions, fragments, and dropped events for each port on the system. RMON statistics collection is activated automatically during system startup, and requires no configuration.

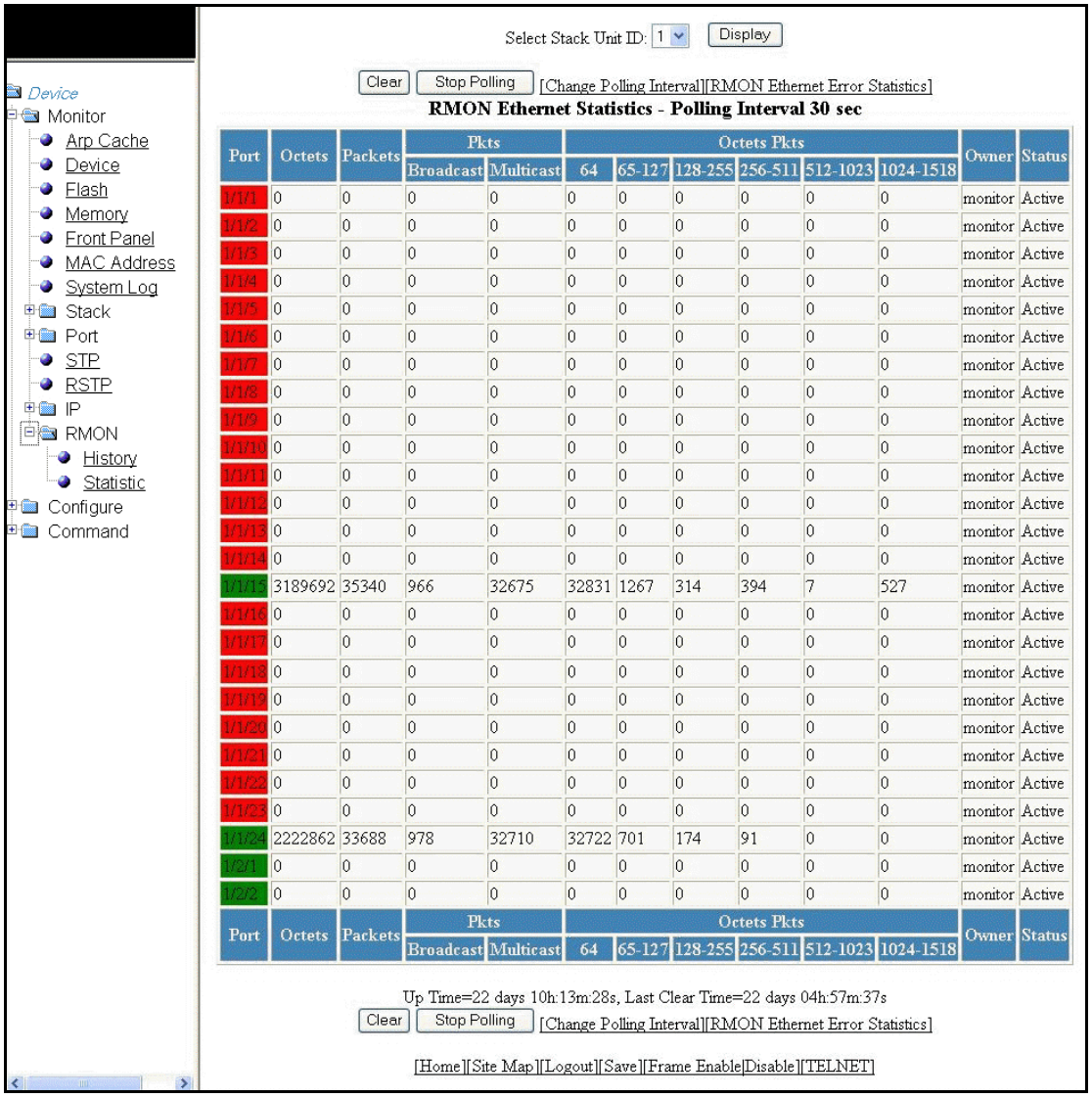
To display RMON statistics, perform the following steps.

1. Click **Monitor** on the left pane and select **RMON**.
2. Click **Statistic**.
3. For Brocade FCX and Brocade ICX 6610 devices, select a stack unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available in the **RMON Ethernet Statistics** window for Brocade FSX devices.

The **RMON Ethernet Statistics** window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 64.

FIGURE 64 Monitoring RMON Ethernet statistics



Port	Octets	Packets	Pkts		Octets Pkts						Owner	Status
			Broadcast	Multicast	64	65-127	128-255	256-511	512-1023	1024-1518		
1/1/1	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/2	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/3	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/4	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/5	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/6	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/7	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/8	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/9	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/10	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/11	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/12	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/13	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/14	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/15	3189692	35340	966	32675	32831	1267	314	394	7	527	monitor	Active
1/1/16	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/17	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/18	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/19	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/20	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/21	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/22	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/23	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/1/24	2222862	33688	978	32710	32722	701	174	91	0	0	monitor	Active
1/2/1	0	0	0	0	0	0	0	0	0	0	monitor	Active
1/2/2	0	0	0	0	0	0	0	0	0	0	monitor	Active
Port	Octets	Packets	Pkts		Octets Pkts						Owner	Status
			Broadcast	Multicast	64	65-127	128-255	256-511	512-1023	1024-1518		

Table 50 describes the fields in the **RMON Ethernet Statistics** window.

TABLE 50 Description of the fields in the **RMON Ethernet Statistics** window

Field	Description
Port	Displays the port number. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Octets	Displays the total number of octets of data received on the network. This number includes octets in bad packets. This number does not include framing bits but does include Frame Check Sequence (FCS) octets.
Packets	Displays the total number of packets received. This number includes bad packets, broadcast packets, and multicast packets.

TABLE 50 Description of the fields in the **RMON Ethernet Statistics** window (Continued)

Field	Description
Packets: Broadcast	Displays the total number of good packets received that were directed to the broadcast address. This number does not include multicast packets.
Packets: Multicast	Displays the total number of good packets received that were directed to a multicast address. This number does not include packets directed to the broadcast address.
Octet Packets: 64	Displays the total number of packets received that were 64 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 65 – 127	Displays the total number of packets received that were from 65 through 127 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 128 – 255	Displays the total number of packets received that were from 128 through 255 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 256 - 511	Displays the total number of packets received that were from 256 through 511 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 512 – 1023	Displays the total number of packets received that were from 512 through 1023 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Octet Packets: 1024 - 1518	Displays the total number of packets received that were from 1024 through 1518 octets long. This number includes bad packets. This number does not include framing bits but does include FCS octets.
Owner	Displays the owner of the packets.
Status	Displays the status of the port.
Up Time	Displays the length of time the device has been available.
Last Clear Time	Displays the length of time data has been accumulating in the current table.

To remove the current data in the table and restart monitoring, click **Clear**. To stop reporting the statistics, click **Stop Polling**,

The **RMON Ethernet Statistics** window contains the following links:

- To change the polling interval, click **Change Polling interval**. For more information, refer to "Changing polling interval" on page 120.
- To display the RMON Ethernet error statistics, click **RMON Ethernet Error Statistics**. For more information, refer to "Displaying RMON Ethernet error statistics" on page 120.

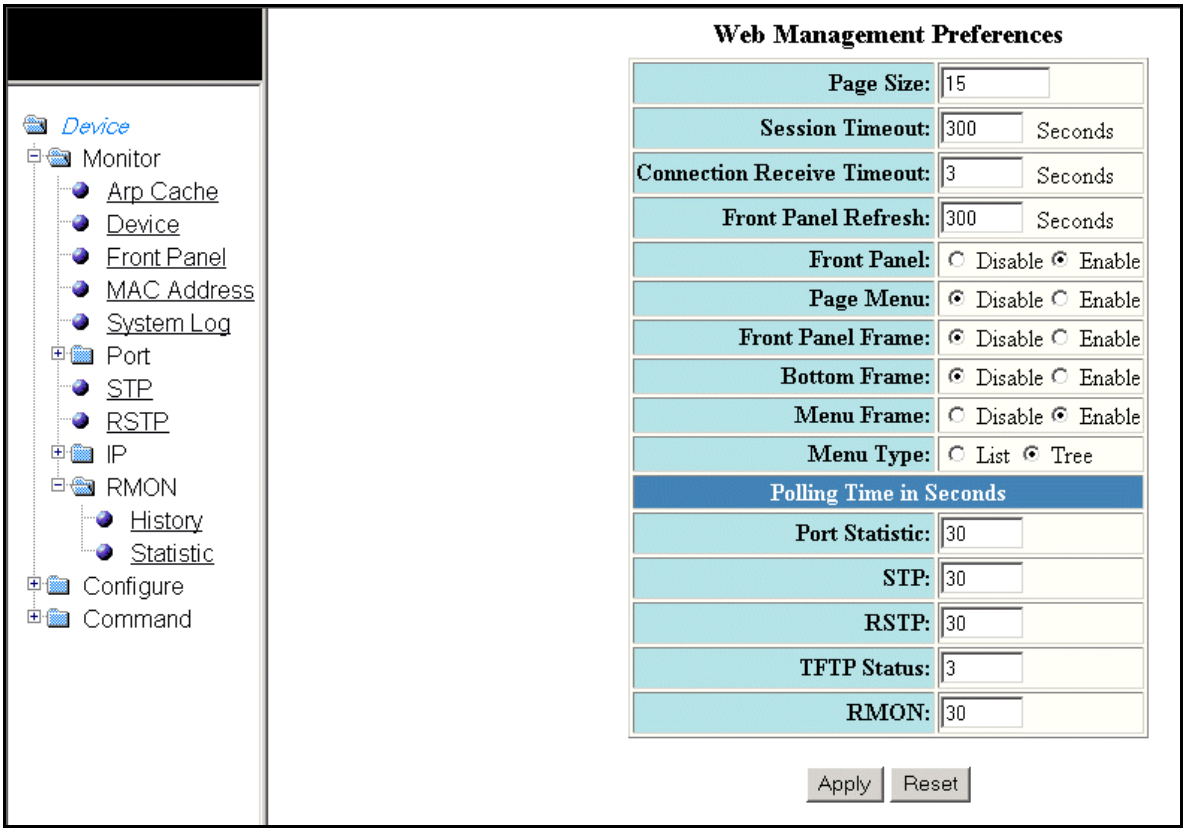
Changing polling interval

To change the number of seconds between reporting the RMON Ethernet statistics, perform the following steps.

1. Click **Change Polling interval** on the **RMON Ethernet Statistics** window.

The **Web Management Preferences** window is displayed as shown in Figure 65.

FIGURE 65 **Modifying web management preferences**



2. Specify the RMON polling interval in the **RMON** field
3. Click **Apply**.

The message **The change has been made** is displayed at the top of the window. To undo the changes, click **Reset**. For more information on web management preferences, refer to "Configuring the web management preference" on page 169.

Displaying RMON Ethernet error statistics

To display RMON error information, perform the following steps.

1. Click **RMON Ethernet Error Statistics** on the **RMON Ethernet Statistics** window.
2. For Brocade FCX and Brocade ICX 6610 devices, select a stack unit ID in the **Select Stack Unit ID** list and click **Display** to view information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available in the **RMON Ethernet Error Statistics** window for Brocade FSX devices.

The **RMON Ethernet Error Statistics** window for Brocade FCX and Brocade ICX 6610 devices is displayed as shown in Figure 66.

FIGURE 66 Monitoring the RMON Ethernet error statistics

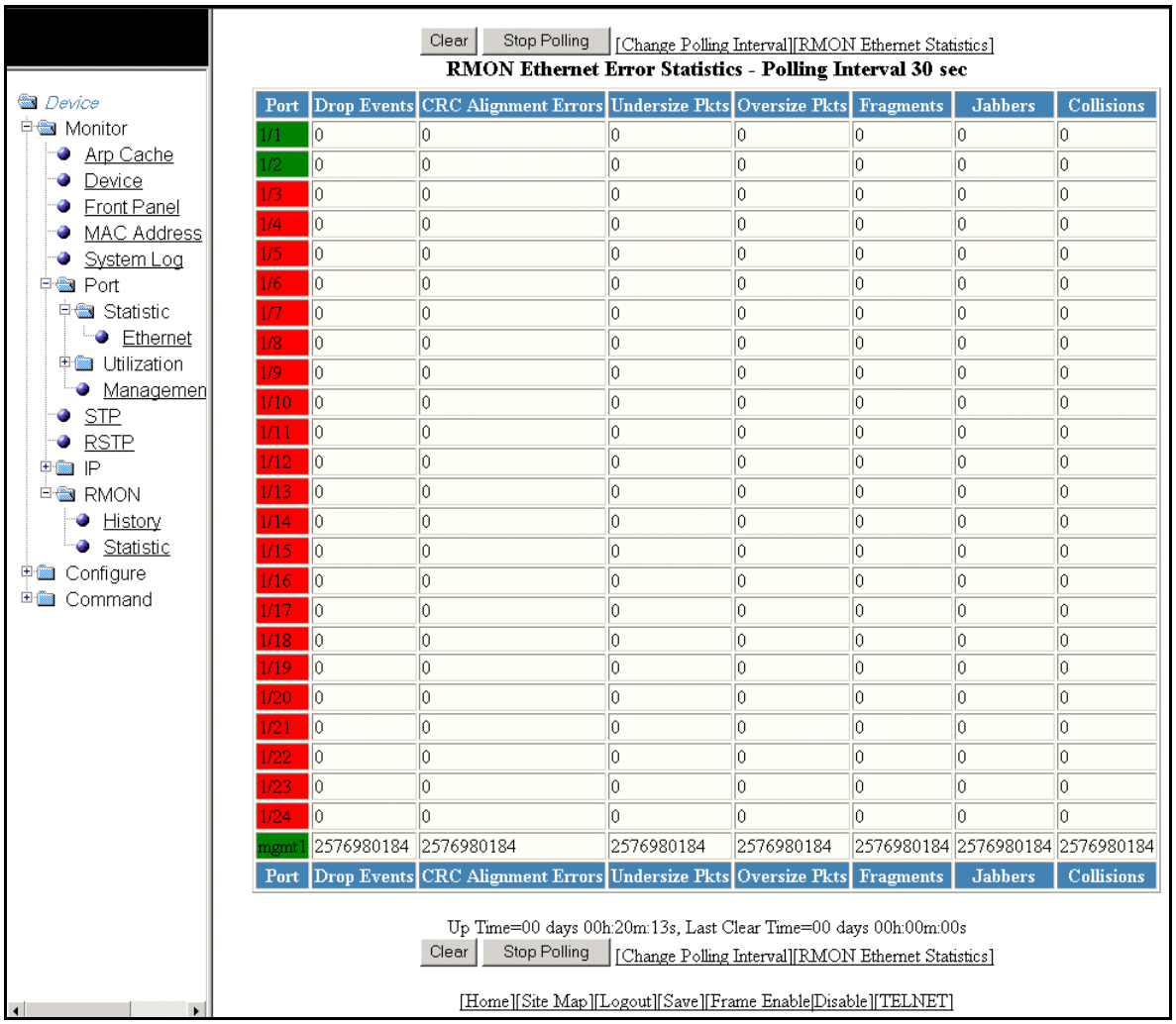

Device
Monitor
Arp Cache
Device
Front Panel
MAC Address
System Log
Port
Statistic
Ethernet
Utilization
Managemen
STP
RSTP
IP
RMON
History
Statistic
Configure
Command
Clear
Stop Polling
[Change Polling Interval][RMON Ethernet Statistics]
RMON Ethernet Error Statistics - Polling Interval 30 sec
Port
Drop Events
CRC Alignment Errors
Undersize Pkts
Oversize Pkts
Fragments
Jabbers
Collisions
1/1 0 0 0 0 0 0 0
1/2 0 0 0 0 0 0 0
1/3 0 0 0 0 0 0 0
1/4 0 0 0 0 0 0 0
1/5 0 0 0 0 0 0 0
1/6 0 0 0 0 0 0 0
1/7 0 0 0 0 0 0 0
1/8 0 0 0 0 0 0 0
1/9 0 0 0 0 0 0 0
1/10 0 0 0 0 0 0 0
1/11 0 0 0 0 0 0 0
1/12 0 0 0 0 0 0 0
1/13 0 0 0 0 0 0 0
1/14 0 0 0 0 0 0 0
1/15 0 0 0 0 0 0 0
1/16 0 0 0 0 0 0 0
1/17 0 0 0 0 0 0 0
1/18 0 0 0 0 0 0 0
1/19 0 0 0 0 0 0 0
1/20 0 0 0 0 0 0 0
1/21 0 0 0 0 0 0 0
1/22 0 0 0 0 0 0 0
1/23 0 0 0 0 0 0 0
1/24 0 0 0 0 0 0 0
mgmt1 2576980184 2576980184 2576980184 2576980184 2576980184 2576980184 2576980184
Port
Drop Events
CRC Alignment Errors
Undersize Pkts
Oversize Pkts
Fragments
Jabbers
Collisions
Up Time=00 days 00h:20m:13s, Last Clear Time=00 days 00h:00m:00s
Clear
Stop Polling
[Change Polling Interval][RMON Ethernet Statistics]
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

Table 51 describes the fields in the **RMON Ethernet Error Statistics** window.

TABLE 51 Description of the fields in the **RMON Ethernet Error Statistics** window

Field	Description
Port	Displays the port number. The port number varies based on the product: • For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum • For Brocade FSX devices – slotnum/portnum
Drop Events	Displays the total number of events in which packets were dropped by the RMON probe due to lack of resources. This number is not necessarily the number of packets dropped, but is the number of times an overrun condition has been detected.

TABLE 51 Description of the fields in the **RMON Ethernet Error Statistics** window (Continued)

Field	Description
CRC Alignment Errors	Displays the total number of packets received that were from 64 through 1518 octets long, but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). The packet length does not include framing bits but does include FCS octets.
Undersize Pkts	Displays the total number of packets received that were less than 64 octets long and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Oversize Pkts	Displays the total number of packets received that were longer than 1518 octets and were otherwise well formed. This number does not include framing bits but does include FCS octets.
Fragments	Displays the total number of packets received that were less than 64 octets long and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). It is normal for this counter to increment, because it counts both runts (which are normal occurrences due to collisions) and noise hits. This number does not include framing bits but does include FCS octets.
Jabbers	Displays the total number of packets received that were longer than 1518 octets and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **NOTE:** This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms. This number does not include framing bits but does include FCS octets.
Collisions	Displays the best estimate of the total number of collisions on this Ethernet segment.
Up Time	Displays the length of time the device has been available.
Last Clear Time	Displays the length of time data has been accumulating in the current table.

To remove the current data in the table and restart monitoring, click **Clear**. To stop reporting the statistics, click **Stop Polling**.

The **RMON Ethernet Error Statistics** window contains the following links:

- To change the polling interval, click **Change Polling interval**. For more information, refer to "Changing polling interval" on page 120.
- To display the RMON statistics, click **RMON Ethernet Statistics**. For more information, refer to "Displaying RMON Ethernet statistics" on page 117.

Section

II

Configuring Device Components

This section describes the **Configure** features, and includes the following chapters:

- Configuring Stack Components 125
- Configuring System Components 133
- Configuring Module Components 171
- Configuring Port Parameters 175
- Configuring Monitor and Mirror Port 181
- Configuring QoS 185
- Configuring VLAN 189
- Configuring STP 201
- Configuring RSTP 207
- Configuring Trunks 213
- Configuring a Static Station 215
- Configuring IP 219
- Configuring OSPF 239
- Configuring RIP 251
- Configuring PIM 261
- Configuring DVMRP 265
- Configuring BGP 271
- Configuring a Virtual Redundant Router 291

Chapter

14

Configuring Stack Components

In this chapter

- Configuring the general settings for an IronStack 125
- Modifying stack priority 126
- Modifying stack ports 128
- Configuring a stack module 129

NOTE
This chapter is specific to Brocade FCX and Brocade ICX 6610 devices.

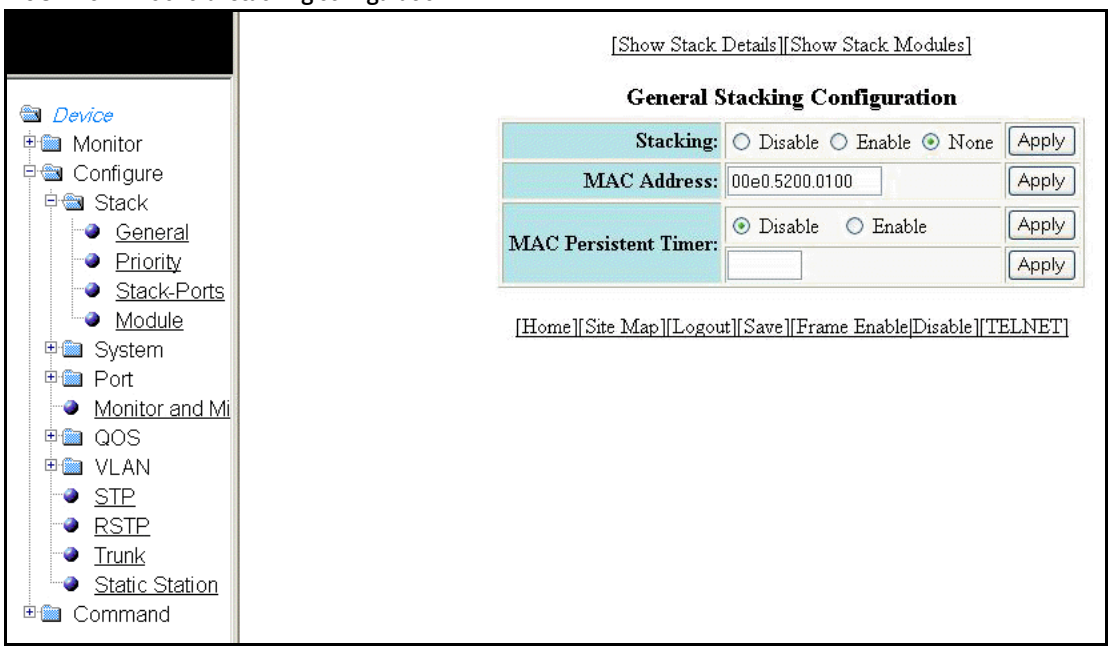
Configuring the general settings for an IronStack

To change the stack settings to improve performance and reliability of the device, perform the following steps.

1. Click **Configure** on the left pane and select **Stack**.
2. Click **General**.

The **General Stacking Configuration** window is displayed as shown in Figure 67.

FIGURE 67 General stacking configuration



3. Click one of the following options for **Stacking** and then click **Apply**:
   - **Disable** - Prevents a unit from sending or listening for any stacking probe messages. In this mode, the unit cannot be forced to join a stack.
   - **Enable** - Enables stacking mode on a new unit before you add it to the stack.
   - **None** - Prevents the unit from actively sending out probe messages; however, the unit can still be called to join a stack by an Active Controller.
4. Enter the Media Access Control (MAC) address of the device in the **MAC Address** field and then click **Apply**.
5. Click **Disable** or **Enable** for **MAC Persistent Timer** and then click **Apply**.

   If you click **Enable**, type the time delay before the stack MAC address changes in the **MAC Persistent Timer** field and then click **Apply**.

The **General Stacking Configuration** window provides links to monitor stack parameters:

- To display the current stack information, click **Show Stack Details**. For more information, refer to "Displaying the stack details" on page 25.
- To display the current information about the stack modules, click **Show Stack Modules**. For more information, refer to "Displaying a stack module" on page 27.

Modifying stack priority

The stack unit with the highest priority is the Active Controller (128 by default). The stack unit with the second highest priority is the Standby Controller, which takes over if the current Active Controller fails.

It is possible to assign the same priority for Active and Standby Controllers, or different priorities (Active highest and Standby second-highest). When the Active and Standby Controllers have the same priority, if the Active Controller fails, the Standby Controller takes over. If the original Active Controller becomes operational again, it will not be able to resume its original role.

When the priorities of the Active and Standby Controllers are different, if the Active Controller fails, the Standby Controller takes over. If the original Active Controller becomes operational again, the old Active Controller regains its role and resets the other units.

You can assign the same priority to the Active and Standby Controllers after the stack is formed. This prevents the intended Standby Controller from becoming the Active Controller during stack construction.

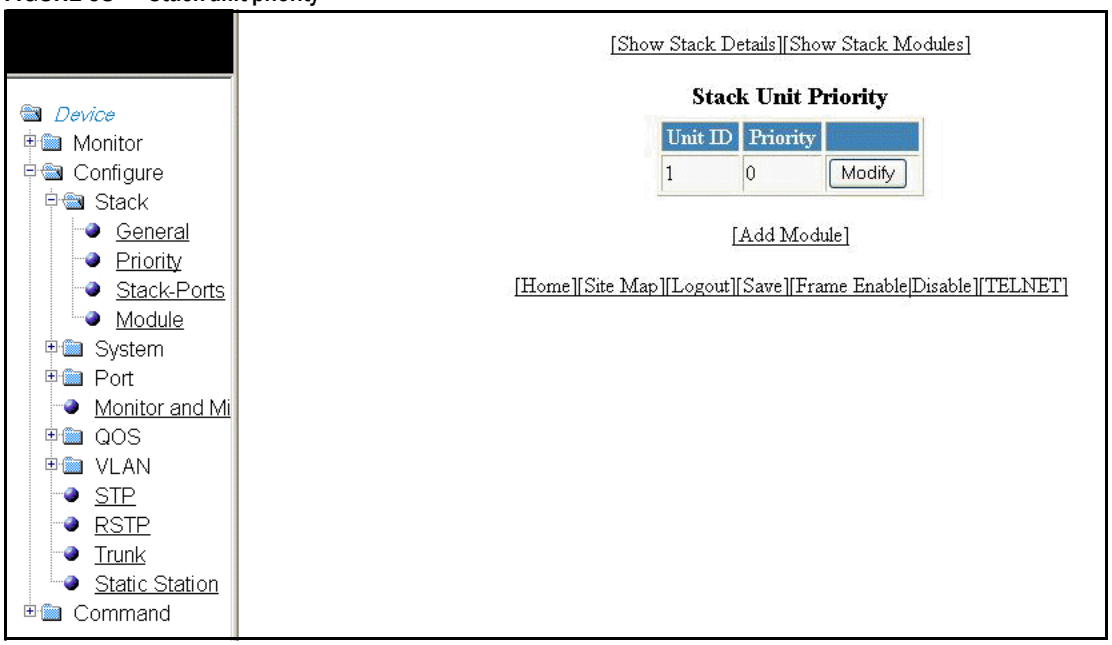
Changing the priority of a stack member triggers an election that takes effect immediately unless the Active Controller's role changes. This change will not take effect until the next stack reload.

To configure the priority of the units within a stack, perform the following steps.

1. Click **Configure** on the left pane and select **Stack**.
2. Click **Priority**.

The **Stack Unit Priority** window is displayed as shown in Figure 68.

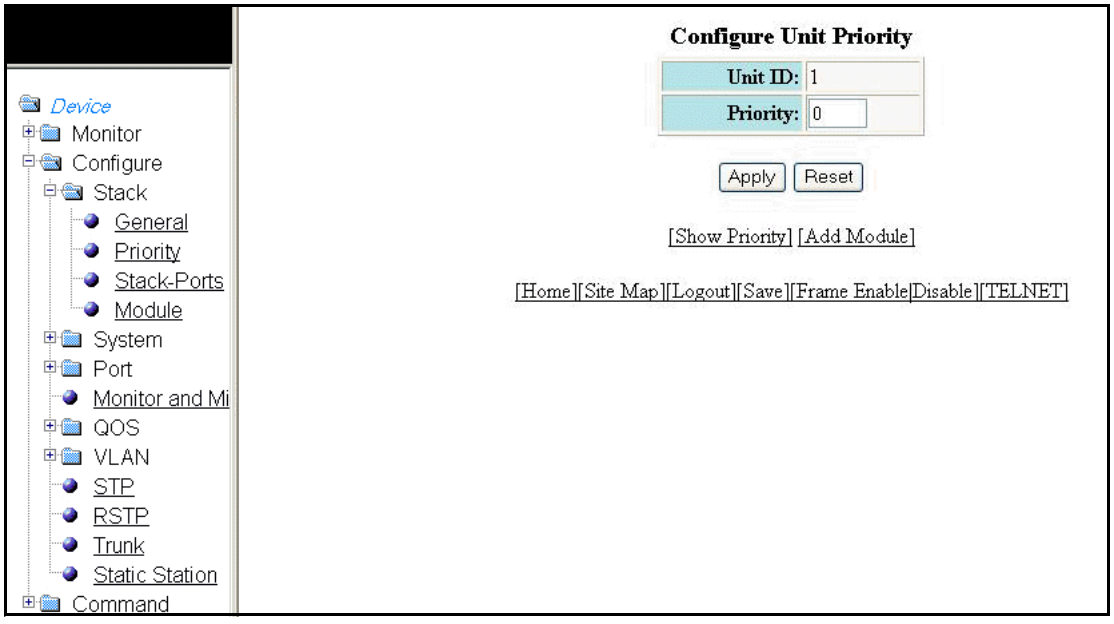
FIGURE 68 Stack unit priority



3. Click **Modify**.

The **Configure Unit Priority** window is displayed as shown in Figure 69.

FIGURE 69 Configuring unit priority



4. Type the priority (from 0 through 255) you want to assign to the stack unit in the **Priority** field.
5. Click **Apply**.

The priority is assigned to the stack unit and the **Stack Unit Priority** window is displayed. To reset the data entered in the configuration pane, click **Reset**.

To display the priority of the stack units, click **Show Priority**. To add a new stack module, click **Add Module**. For more information on how to configure a stack module, refer to "Configuring a stack module" on page 129.

Modifying stack ports

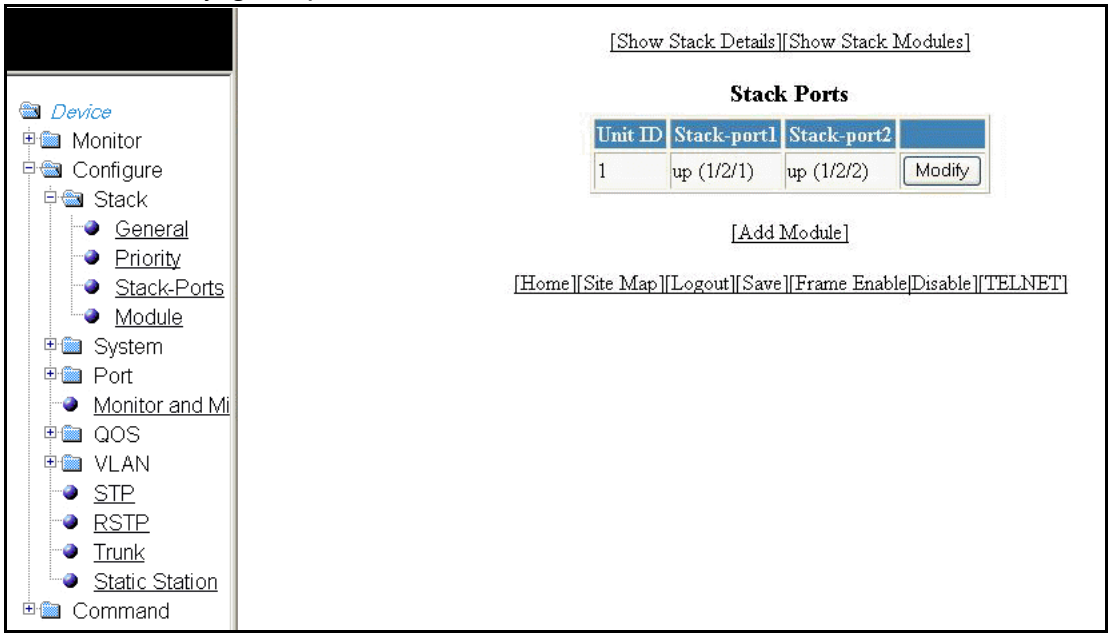
NOTE
You cannot change the stack ports for the Brocade ICX 6610 device.

To modify the stack ports, perform the following steps.

1. Click **Configure** on the left pane and select **Stack**.
2. Click **Stack-Ports**.

The **Stack Ports** window is displayed as shown in Figure 70.

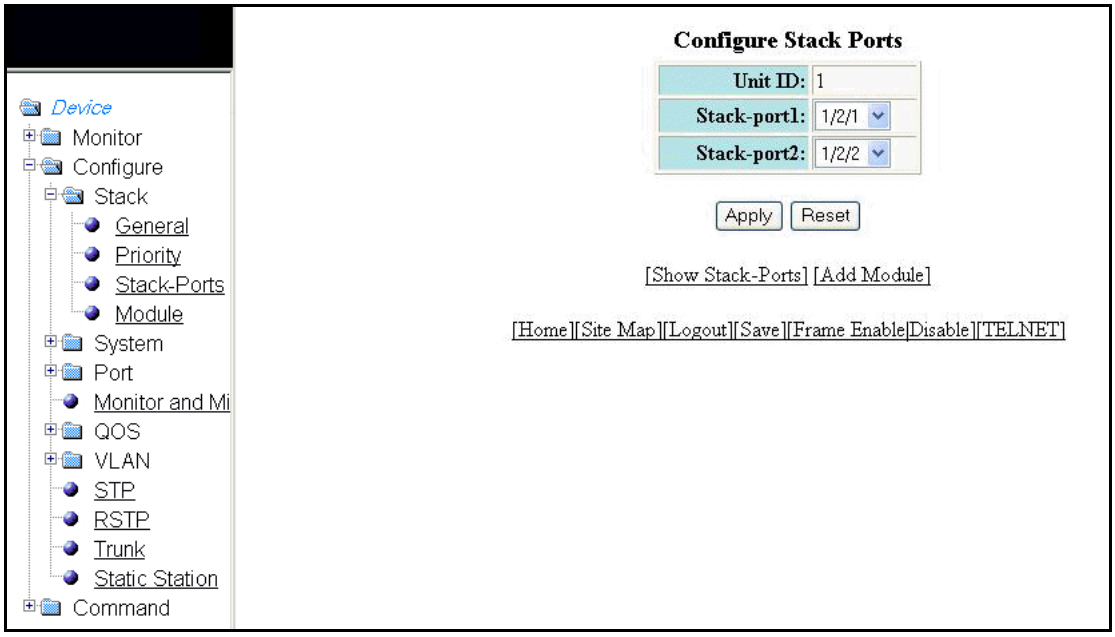
FIGURE 70 Modifying stack ports



3. Click **Modify**.

The **Configure Stack Ports** window is displayed as shown in Figure 71.

FIGURE 71 Modifying stack ports



4. Select a port in the **Stack-port1** list.
5. Select a port in the **Stack-port2** list.
6. Click **Apply**.

The stack ports are modified and the **Stack Ports** window is displayed as shown in Figure 70.

To reset the data entered in the configuration pane, click **Reset**. To display the configured stack port, click **Show Stack-Ports**.

To configure a stack module, click **Add Module**. For more information on how to configure a stack module, refer to "Configuring a stack module" on page 129.

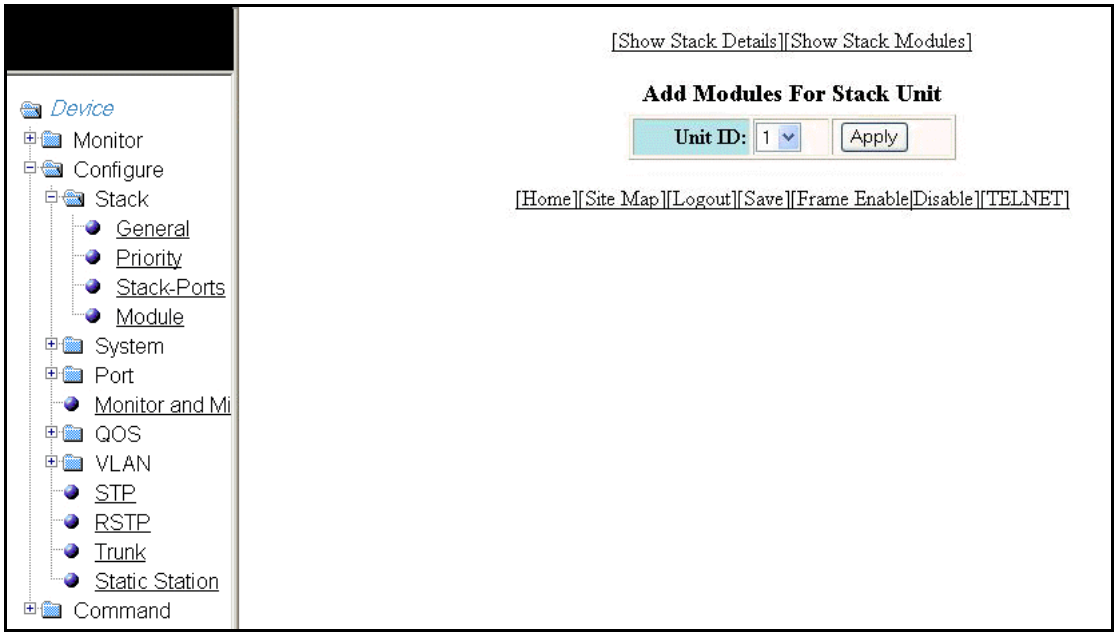
Configuring a stack module

To configure a stack module, perform the following steps.

1. Click **Configure** on the left pane and select **Stack**.
2. Click **Module**.

The **Add Modules For Stack Unit** window is displayed as shown in Figure 72.

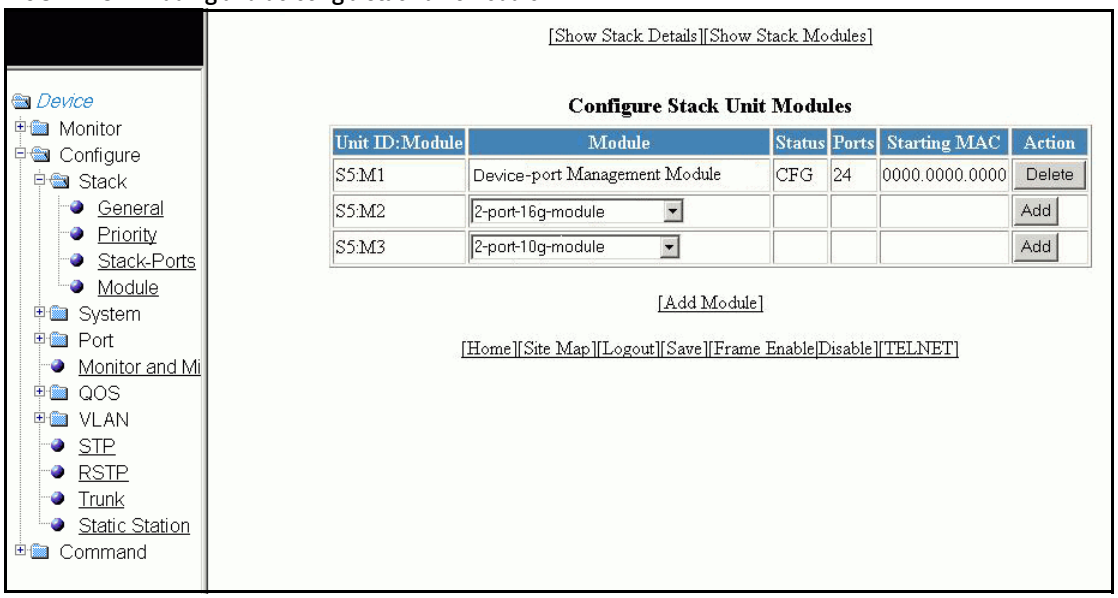
FIGURE 72 Adding modules for a stack unit



3. Select a stack unit identifier in the **Unit ID** list.
4. Click **Apply**.

The **Configure Stack Unit Modules** window is displayed as shown in Figure 73.

FIGURE 73 Adding and deleting a stack unit module



5. Select a stack module in the list on the **Module** column and then click **Add**.

To display current stack details, stack port status, and stack neighbors information, click **Show Stack Details**. For more information, refer to "Displaying the stack details" on page 25. Click **Delete** to delete a stack unit module. You cannot delete the active modules.

To display the stack unit modules, click **Show Stack Modules**. For more information, refer to "Displaying a stack module" on page 27.

Chapter

15

Configuring System Components

In this chapter

- Configuring the system boot sequence for Brocade FCX and Brocade ICX 6610 devices 134
- Configuring the system boot sequence for Brocade FSX devices 135
- Configuring the system clock 136
- Configuring the general system settings 137
- Configuring the system identification. 139
- Configuring the system IP address. 140
- Configuring a standard ACL 141
- Configuring an extended ACL 142
- Configuring an IP access group 144
- Configuring the system MAC filter 145
- Configuring the maximum system parameter value 148
- Configuring a system module 149
- Configuring an NTP server 151
- Configuring a RADIUS server 152
- Configuring a TACACS/TACACS+ server 154
- Configuring management authentication 155
- Configuring management authorization 156
- Configuring management accounting 157
- Configuring an SNMP community string 158
- Configuring the general management parameters. 160
- Configuring a management system log 161
- Configuring a trap 164
- Configuring a trap receiver 166
- Configuring a management user account 168
- Configuring the web management preference 169

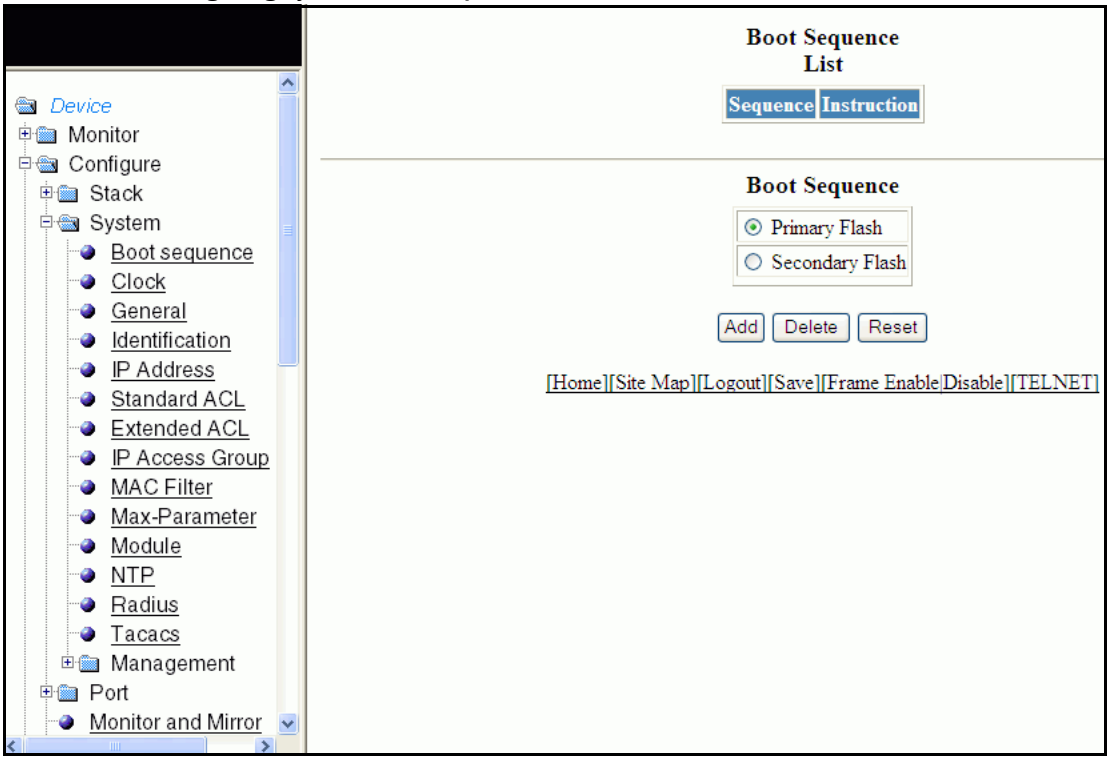
Configuring the system boot sequence for Brocade FCX and Brocade ICX 6610 devices

To configure the system boot sequence for Brocade FCX and Brocade ICX 6610 devices, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Boot sequence**.

The **Boot Sequence** window is displayed as shown in Figure 74.

FIGURE 74 **Configuring system boot sequence for Brocade FCX and Brocade ICX 6610 devices**



3. There are two types of boot sequence operations:
   - Click **Primary Flash** to store the image files and configuration files in the local storage device. By default, **Primary Flash** is enabled.
   - Click **Secondary Flash** to store the redundant images for additional reload reliability or to preserve one software image while testing another one.
4. Click **Add**.

The message **The change has been made** is displayed and the boot sequence is listed in the **Boot Sequence List** pane.

To reset the data entered in the configuration pane, click **Reset**. You can also delete the boot sequence operation by clicking **Delete**.

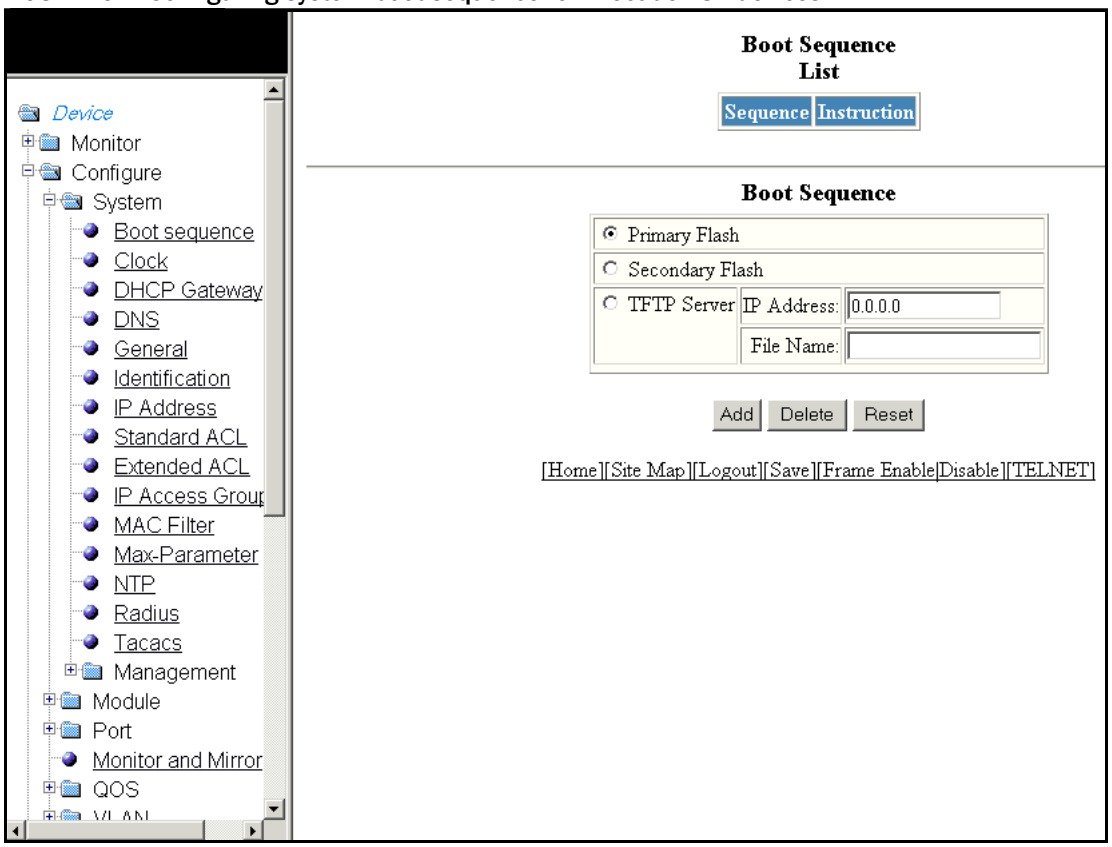
Configuring the system boot sequence for Brocade FSX devices

To configure the system boot sequence for Brocade FSX devices, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Boot sequence**.

The **Boot Sequence** window is displayed as shown in Figure 75.

FIGURE 75 Configuring system boot sequence for Brocade FSX devices



3. There are three types of boot sequence operations:
   - Click **Primary Flash** to store the image files and configuration files in the local storage device. By default, **Primary Flash** is enabled.
   - Click **Secondary Flash** to store the redundant images for additional reload reliability or to preserve one software image while testing another one.
   - Click **TFTP Server** to store configuration files to a TFTP server. Provide the following information:
     - **IP Address** – Type the IP address of the TFTP server.
     - **File Name** – Type the file name.
4. Click **Add**.

The message **The change has been made** is displayed and the boot sequence is listed in the **Boot Sequence List** pane.

To reset the data entered in the configuration pane, click **Reset**. You can also delete the boot sequence operation by clicking **Delete**.

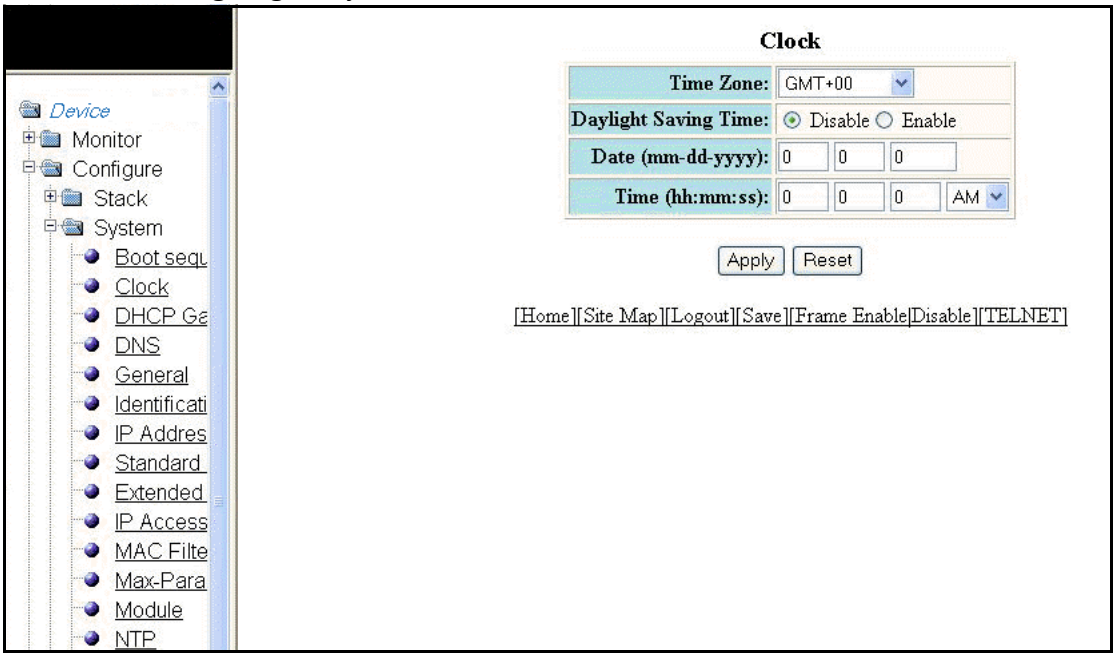
Configuring the system clock

To configure the system clock, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Clock**.

The **Clock** window is displayed as shown in Figure 76.

FIGURE 76 Configuring the system clock



3. Select the GMT time zone that you want to configure for the device in the **Time Zone** list.
4. Click **Disable** or **Enable** for **Daylight Saving Time**. Daylight Saving Time applies to the US time zone only.
5. Type the date in mm-dd-yyyy format in the **Date (mm-dd-yyyy)** field.
6. Type the time in hh:mm:ss format in the **Time (hh:mm:ss)** field and select **AM** or **PM** in the list.
7. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

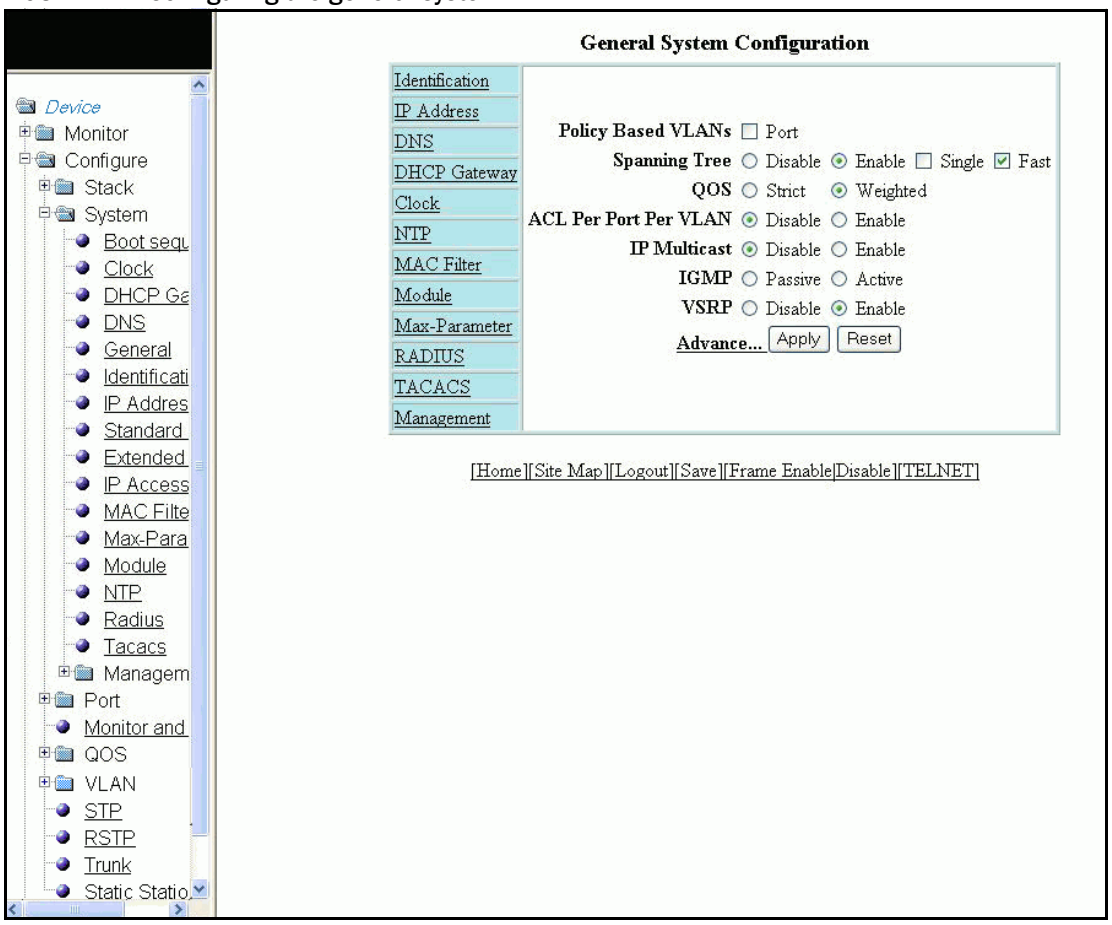
Configuring the general system settings

To configure the general system settings, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **General**.

The **General System Configuration** window is displayed as shown in Figure 77.

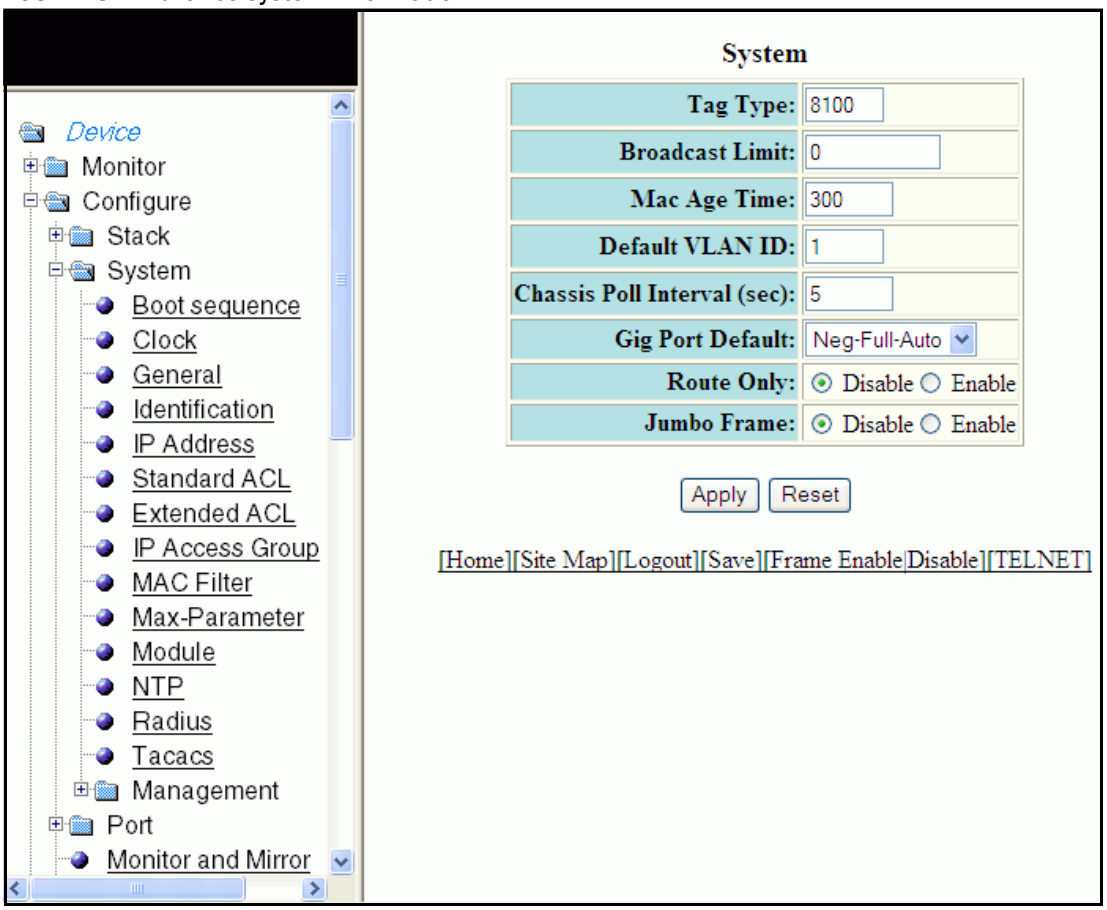
FIGURE 77 Configuring the general system



3. Select the **Port** check box for **Policy based VLANs** to enable configuration of port-based VLANs.
4. Click **Disable** or **Enable** for **Spanning Tree**. If you click **Enable**, select the **Single** or **Fast** check box.
5. Click **Strict** or **Weighted** for **QOS**.
6. Click **Disable** or **Enable** for **ACL Per Port Per VLAN**.
7. Click **Disable** or **Enable** for **IP Multicast**.
8. Click **Passive** or **Active** for **IGMP**.
9. Click **Disable** or **Enable** for **VSRP**.
10. To configure additional system parameters, click **Advance**.

The **System** window is displayed as shown in Figure 78.

FIGURE 78 Advance system information



11. Type the VLAN tag type in hexadecimal format from zero through ffff in the **Tag Type** field. The default is 0081.
12. Type the total number of broadcast packets or bytes that can be allowed on the port in the **Broadcast Limit** field.
13. Type the number of seconds a port address remains active in the address table in the **Mac Age Time** field.
14. Type the default VLAN ID number in the **Default VLAN ID** field.
15. Type the interval, in seconds, in which the chassis is polled in the **Chassis Poll Interval (sec)** field.
16. Select a negotiation mode in the **Gig Port Default** list.
17. Click **Disable** or **Enable** for **Route Only**. If you click **Enable**, Layer 2 switching is disabled globally.
18. Click **Disable** or **Enable** for **Jumbo Frame**.

    Jumbo frames are Ethernet frames with more than 1,500 bytes MTU.
19. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

The **General System Configuration** window provides the following links to configure the system parameters:

- **Identification**
- **IP Address**
- **DNS**
- **DHCP Gateway**
- **Clock**
- **NTP**
- **MAC Filter**
- **Module**
- **Max-Parameter**
- **RADIUS**
- **TACACS**
- **Management**

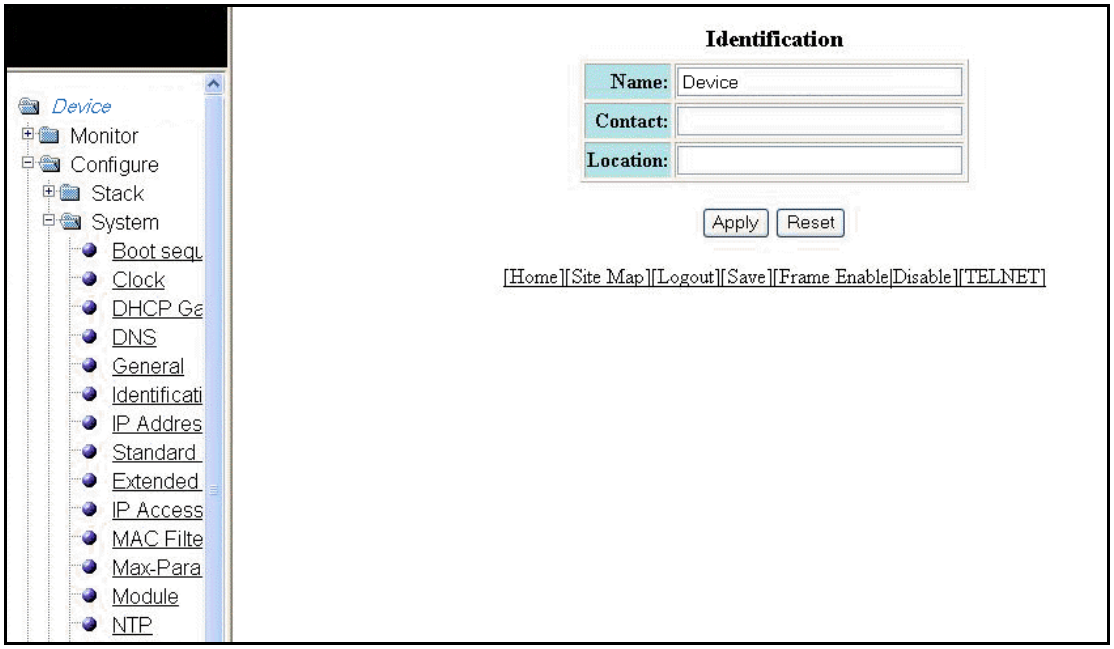
Configuring the system identification

To configure the system identification information, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Identification**.

The **Identification** window is displayed as shown in Figure 79.

FIGURE 79 Configuring the system identification



3. Type the name of the device in the **Name** field.
4. Type the contact information of the device in the **Contact** field.
5. Type the location of the device in the **Location** field.
6. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

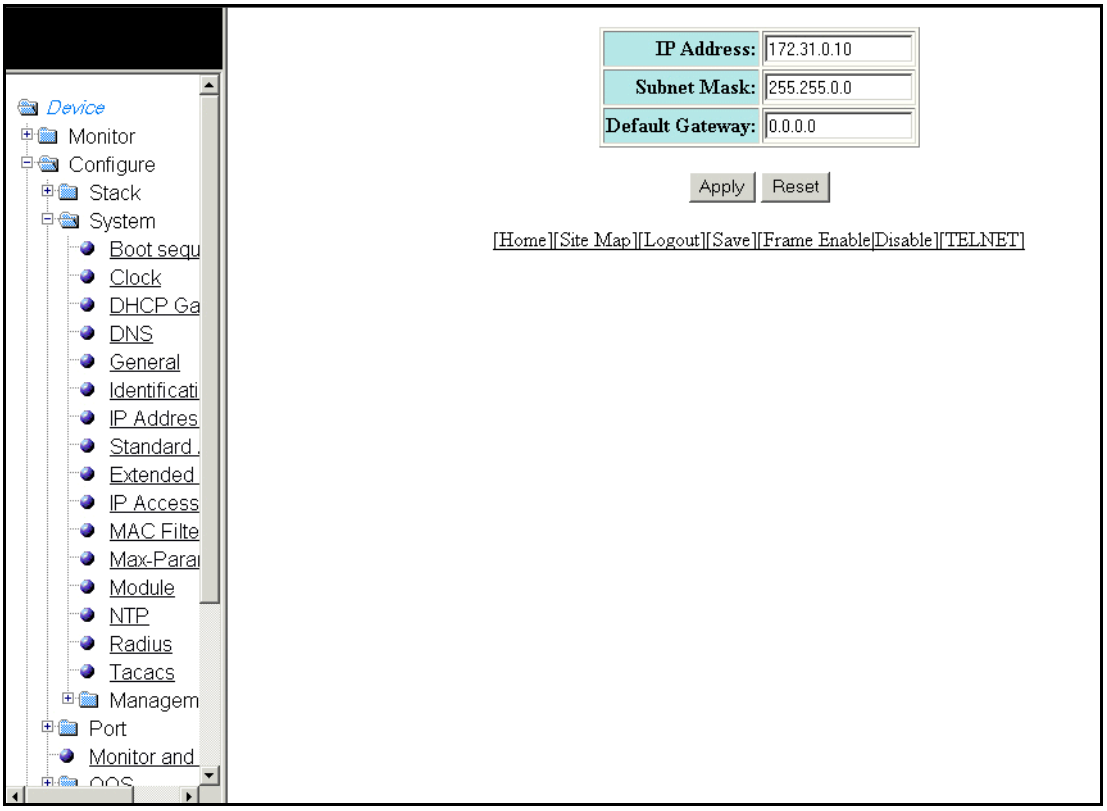
Configuring the system IP address

To configure the IP address of the system, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **IP Address**.

The IP address window is displayed as shown in Figure 80.

FIGURE 80 Configuring the system IP address



3. Type the IP address of the device in the **IP Address** field.
4. Type the network mask for the IP address in the **Subnet Mask** field.
5. Type the IP address of a locally attached Layer 3 switch (or a Layer 3 switch attached to the Layer 2 switch by bridges or other Layer 2 switches) in the **Default Gateway** field.
6. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

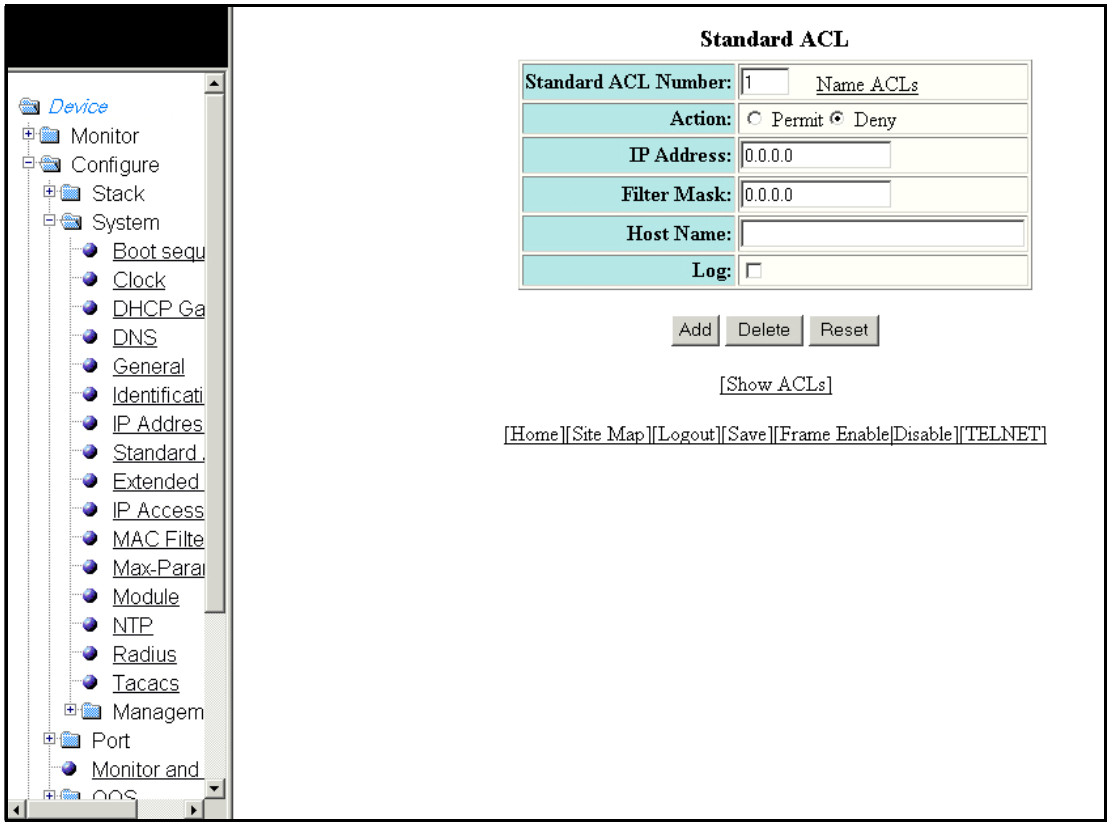
Configuring a standard ACL

To configure a standard Access Control List (ACL), perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Standard ACL**.

The **Standard ACL** window is displayed as shown in Figure 81.

FIGURE 81 Configuring a standard ACL



3. Type the standard ACL number from 1 through 99 in the **Standard ACL Number** field. If you want to type an ACL name, click **Name ACLs**. The field label changes to **Standard ACL Name**.
4. Click **Permit** or **Deny** for **Action** so that the ACL forwards or drops the packets that match the policy in the access list.
5. Type the IP address of the route's destination in the **IP Address** field.
6. Type the masking bits in the **Filter Mask** field. This allows you to specify a range of IP addresses to include or exclude based on mask matching.
7. Type the host name in the **Host Name** field. The host name enables you to perform Telnet, ping, and trace route commands.
8. Select the **Log** check box to log the entries.

9. Click **Add**.

The message **The change has been made** is displayed. To display the configured standard ACL, click **Show ACLs**. To delete the configured ACL, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

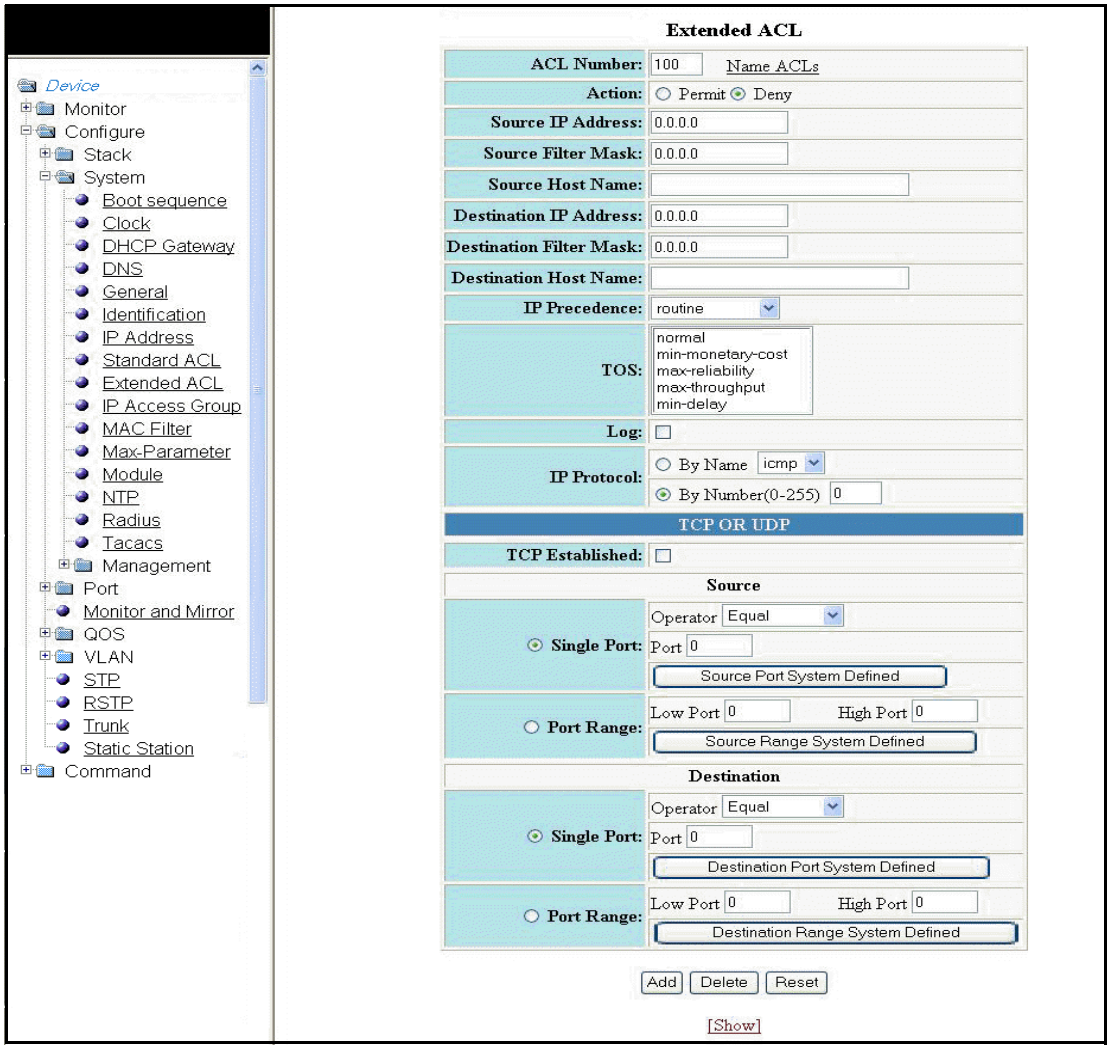
Configuring an extended ACL

To configure an extended Access Control List (ACL), perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Extended ACL**.

The **Extended ACL** window is displayed as shown in Figure 82.

FIGURE 82 Configuring an extended ACL



3. Type the extended access list number from 100 through 199 in the **ACL Number** field. If you want to specify an extended access list name, click **Name ACLs**. The field label changes to **ACL Name**.

4. Click **Permit** or **Deny** for **Action** so that the packets that match the policy are forwarded or dropped.
5. Type the source IP address in the **Source IP Address** field.
6. Type the source mask in the **Source Filter Mask** field.
7. Type the source host name in the **Source Host Name** field.
8. Type the destination IP address in the **Destination IP Address** field.
9. Type the destination mask in the **Destination Filter Mask** field.
10. Type the destination host name in the **Destination Host Name** field.
11. Select one of the following options in the **IP Precedence** list:
    - **routine** – The ACL matches packets that have the routine precedence.
    - **priority** – The ACL matches packets that have the priority precedence.
    - **immediate** – The ACL matches packets that have the immediate precedence.
    - **flash** – The ACL matches packets that have the flash precedence.
    - **flash-override** – The ACL matches packets that have the flash override precedence.
    - **critical** – The ACL matches packets that have the critical precedence.
    - **internet** – The ACL matches packets that have the internetwork control precedence.
    - **network** – The ACL matches packets that have the network control precedence.
12. Select one of the following options in the **TOS** list:
    - **normal** – The ACL matches packets that have the normal Type of Service (ToS).
    - **min-monetary-cost** – The ACL matches packets that have the minimum monetary cost ToS.
    - **max-reliability** – The ACL matches packets that have the maximum reliability ToS.
    - **max-throughput** – The ACL matches packets that have the maximum throughput ToS.
    - **min-delay** – The ACL matches packets that have the minimum delay ToS.
13. Select the **Log** check box to enable generation of SNMP traps and syslog messages for packets denied by the ACL.
14. Click **By Name** for IP **Protocol** to select the IP protocol by name or click **By Number** to specify the number (from 0 through 255).
15. Select the **TCP Established** check box so that the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to “1”) in the Control Bits field of the TCP packet header. The policy applies only to the established TCP sessions, not to the new sessions.

    NOTE
    This field applies only to the destination TCP ports, not the source TCP ports.

16. Enter the following information for **Source**:
    a. To configure a single port, click **Single Port**.
        i. Select one of the following options for **Operator**:
        - **Equal** - The policy applies to the TCP or UDP port number or name you enter.

- **NotEqual** - The policy applies to all the TCP or UDP port numbers except the port number or port name you enter.
- **LessThan** - The policy applies to the TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter.
- **GreaterThan** - The policy applies to the TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter.

ii. Click **Source Port System Defined**.

b. To configure a range of ports, click **Port Range**.

i. Type the lower port number in the **Low Port** field and the highest port number in the **High Port** field.

ii. Click **Source Range System Defined**.

17. To configure the destination port settings under **Destination**, follow the procedure explained in step 16.
18. Click **Add**.

The message **The change has been made** is displayed. To display the configured extended numbered ACL, click **Show**.

To delete the configured extended numbered ACL, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

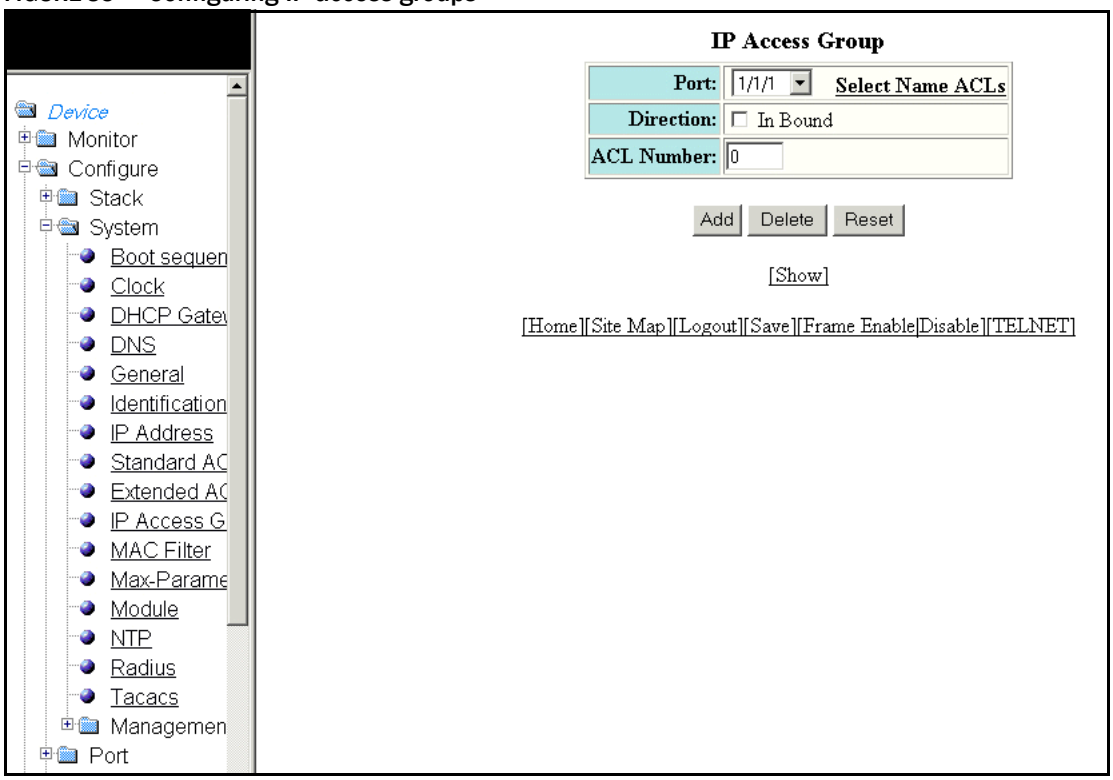
Configuring an IP access group

To configure an IP access group, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **IP Access Group**.

The **IP Access Group** window is displayed as shown in Figure 83.

FIGURE 83 Configuring IP access groups



3. Select a port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Select the **In Bound** check box for **Direction** to enable incoming traffic on the interface to which you apply the ACL.
5. Type the access list number in the **ACL Number** list. If you want to type access list name, click **Select Name ACLs**. The field label changes to **ACL Name**. Now, you can type the access list name up to 256 alphanumeric characters.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured IP access group, click **Show**.

To delete the configured IP access group, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

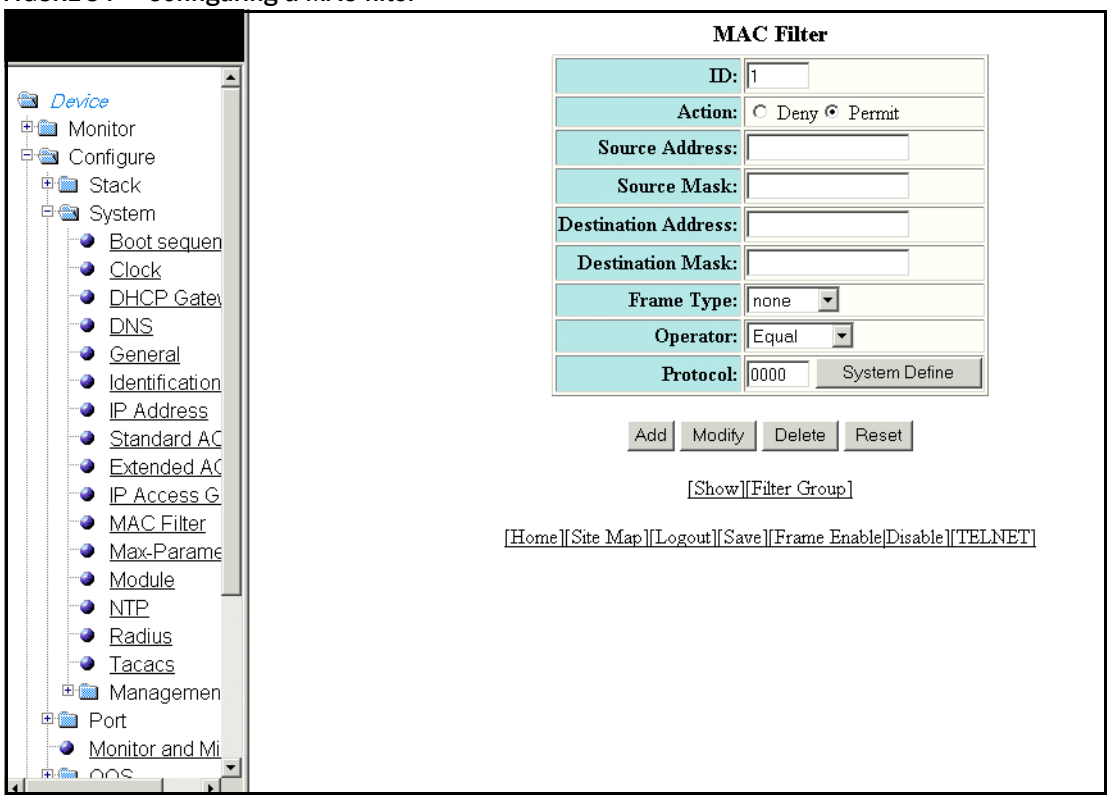
Configuring the system MAC filter

To configure the system MAC filter, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **MAC Filter**.

The **MAC Filter** window is displayed as shown in Figure 84.

FIGURE 84 Configuring a MAC filter



3. Type the filter number in the **ID** field.
4. Click **Deny** or **Permit** for **Action**.
5. Type the source MAC address in xx.xx.xx.xx.xx.xx format in the **Source Address** field.
6. Type the source mask in the **Source Mask** field.
7. Type the destination MAC address in xx.xx.xx.xx.xx.xx format in the **Destination Address** field.
8. Type the destination mask in the **Destination Mask** field.
9. Select the type of frame in the **Frame Type** list.

NOTE
The **Frame Type** list is not available in the **MAC Filter** window for Brocade FSX devices.

10. Select the comparison operator in the **Operator** list.

NOTE
The **Operator** list is not available in the **MAC Filter** window for Brocade FSX devices.

11. Type the protocol identifier in the **Protocol** field. To select the system-defined protocol, click **System Define**.

NOTE
The **Protocol** field is not available in the **MAC Filter** window for Brocade FSX devices.

12. Click **Add**.

The message **The change has been made** is displayed. To display the configured MAC filter, click **Show**.

To change the configured MAC filter, click **Modify**. You can also delete the MAC filter by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

To configure a filter group, click **Filter Group**. For more information on how to configure a filter group, refer to "Configuring a filter group" on page 147.

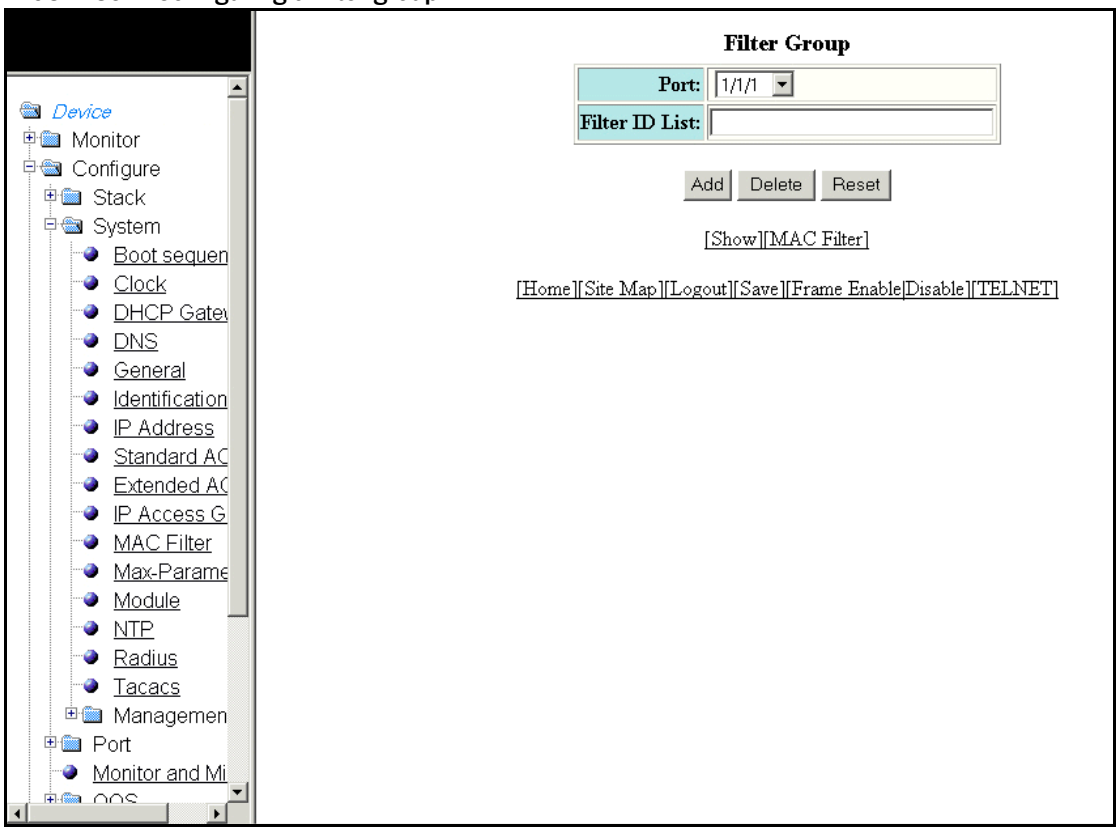
Configuring a filter group

To configure a system filter group, perform the following steps.

1. Click **Filter Group** on the right pane of the **MAC Filter** window.

The **Filter Group** window is displayed as shown in Figure 85.

FIGURE 85 Configuring a filter group



2. Select a port number in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
3. Type the filter identifier in the **Filter ID List** field.
4. Click **Add**.

The message **The change has been made** is displayed. To display the configured filter group, click **Show**.

To delete the configured filter group, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

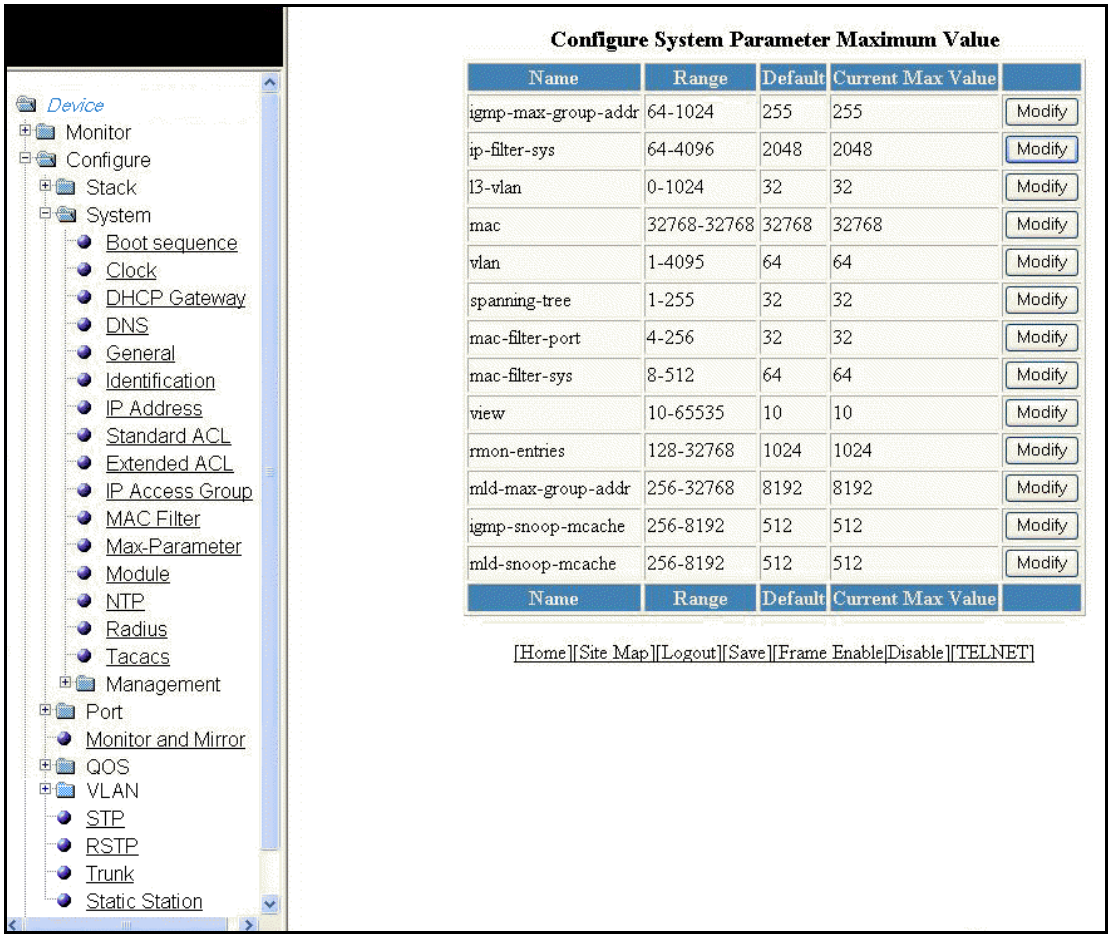
Configuring the maximum system parameter value

To configure the maximum system parameter value, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Max-Parameter**.

The **Configure System Parameter Maximum Value** window is displayed as shown in Figure 86.

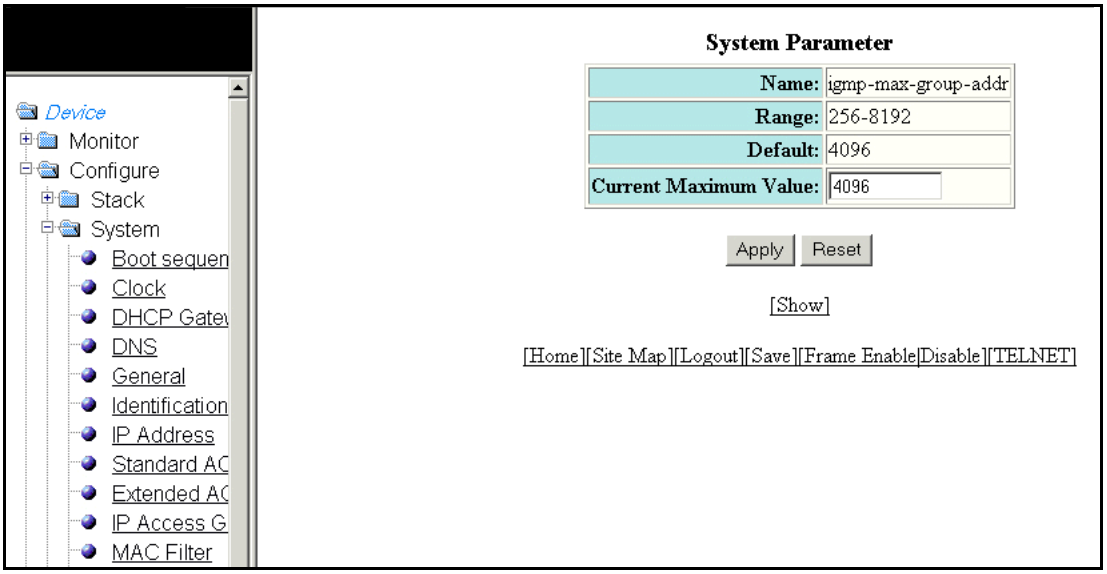
FIGURE 86 Configuring the maximum system parameter



3. To change the values for each system parameter, click **Modify**.

The **System Parameter** window is displayed as shown in Figure 87.

FIGURE 87 Modifying the maximum parameter value



4. Type the maximum value in the **Current Maximum Value** field.
5. Click **Apply**.

The message **The change has been made** is displayed. To display the configured maximum system value, click **Show**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a system module

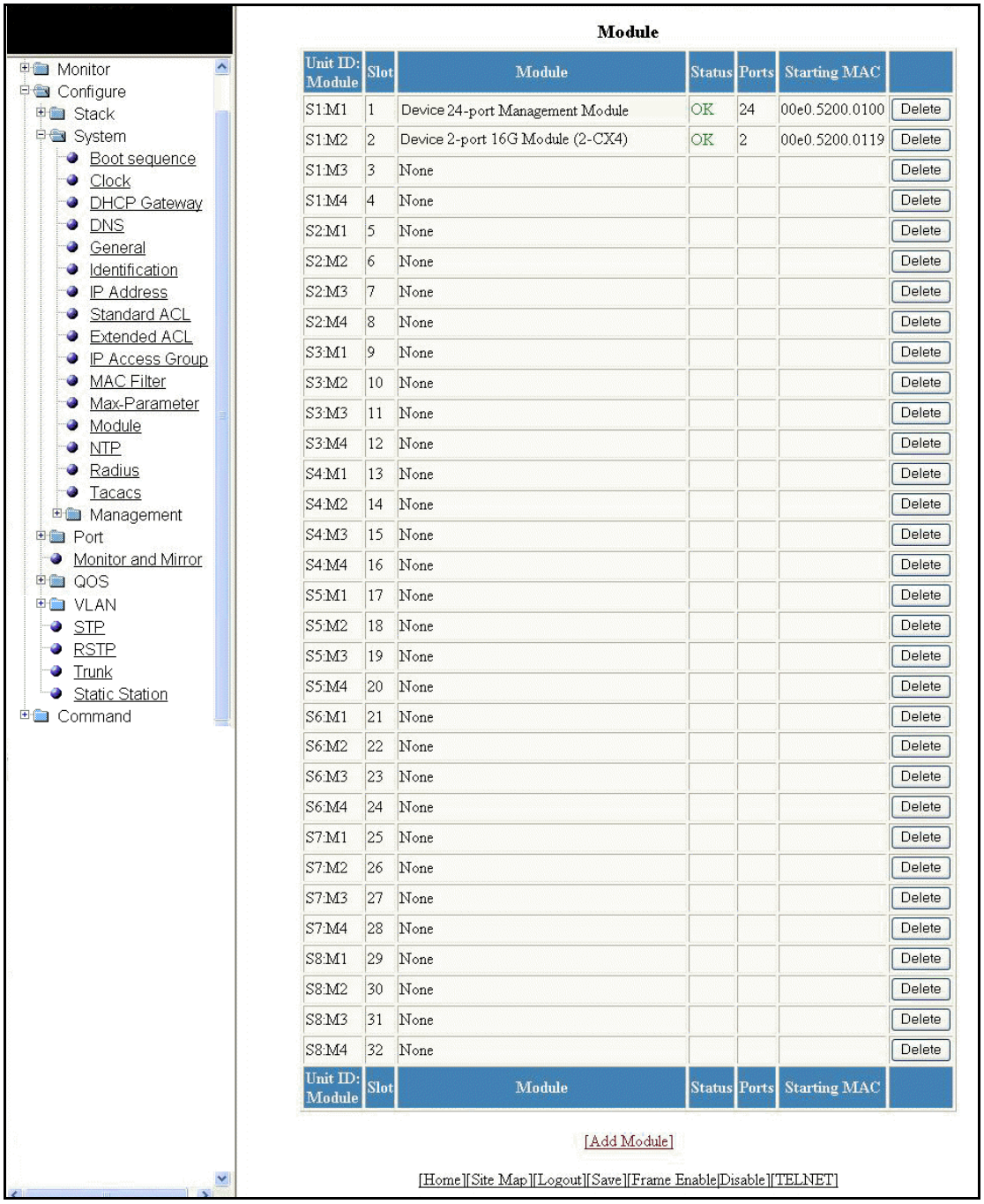
NOTE
This system module is specific to Brocade FCX and Brocade ICX 6610 devices and is not available for Brocade FSX devices.

To configure a system module, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Module**.

The **Module** window is displayed as shown in Figure 88.

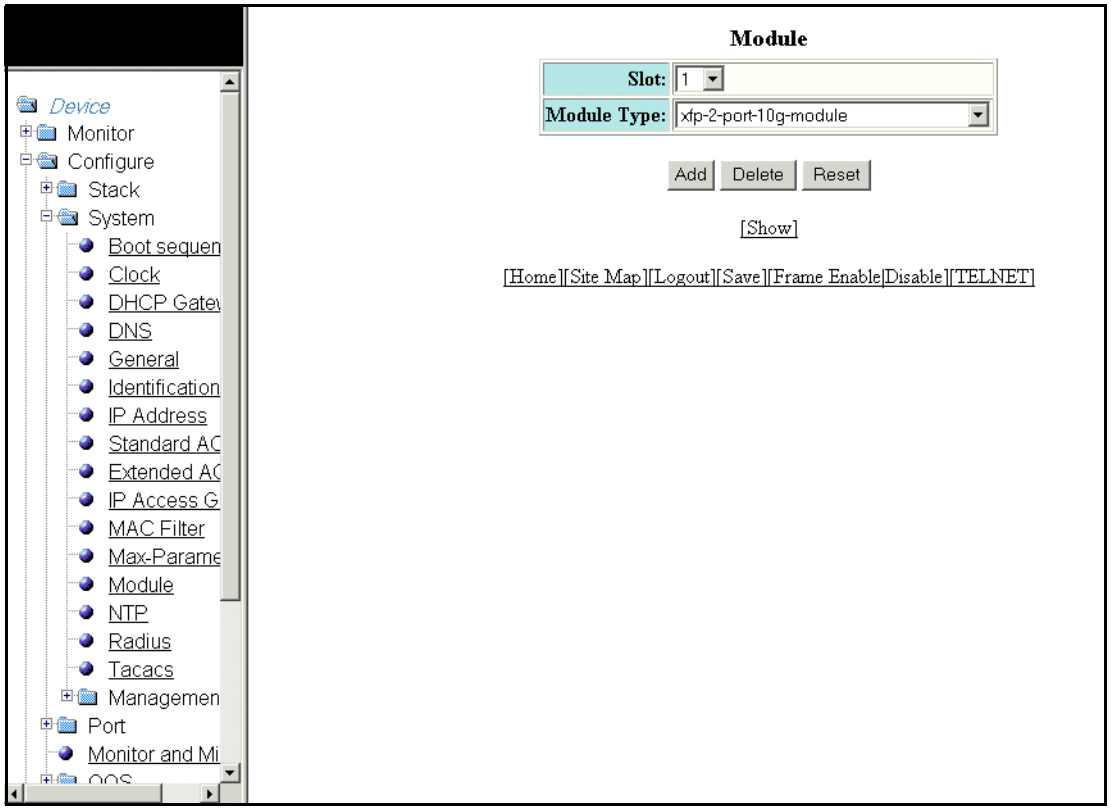
FIGURE 88 Configuring system modules



3. Click **Add Module**.

The **Module** window is displayed as shown in Figure 89.

FIGURE 89 Adding system modules



4. Select a slot number in the **Slot** list.
5. Select a chassis module type in the **Module Type** list.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured module, click **Show**.

To delete the configured module, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

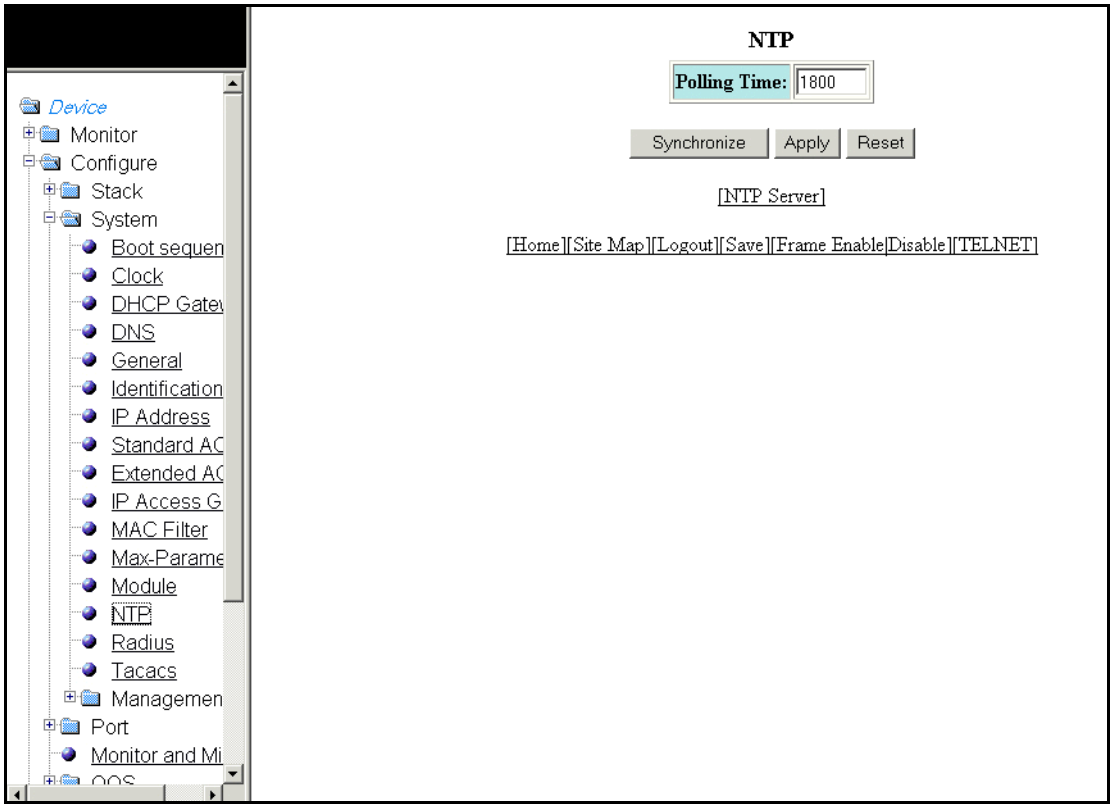
Configuring an NTP server

To configure a Network Transfer Protocol (NTP) server, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **NTP**.

The **NTP** window is displayed as shown Figure 90.

FIGURE 90 Configuring an NTP server



3. Type the minimum poll interval for the NTP messages in the **Polling Time** field.
4. Click **Synchronize** so that system is synchronized to an NTP peer or click **Apply** to save your configuration.

The message **The change has been made** is displayed. To display the configured NTP server, click **NTP Server**. To reset the data entered in the configuration pane, click **Reset**.

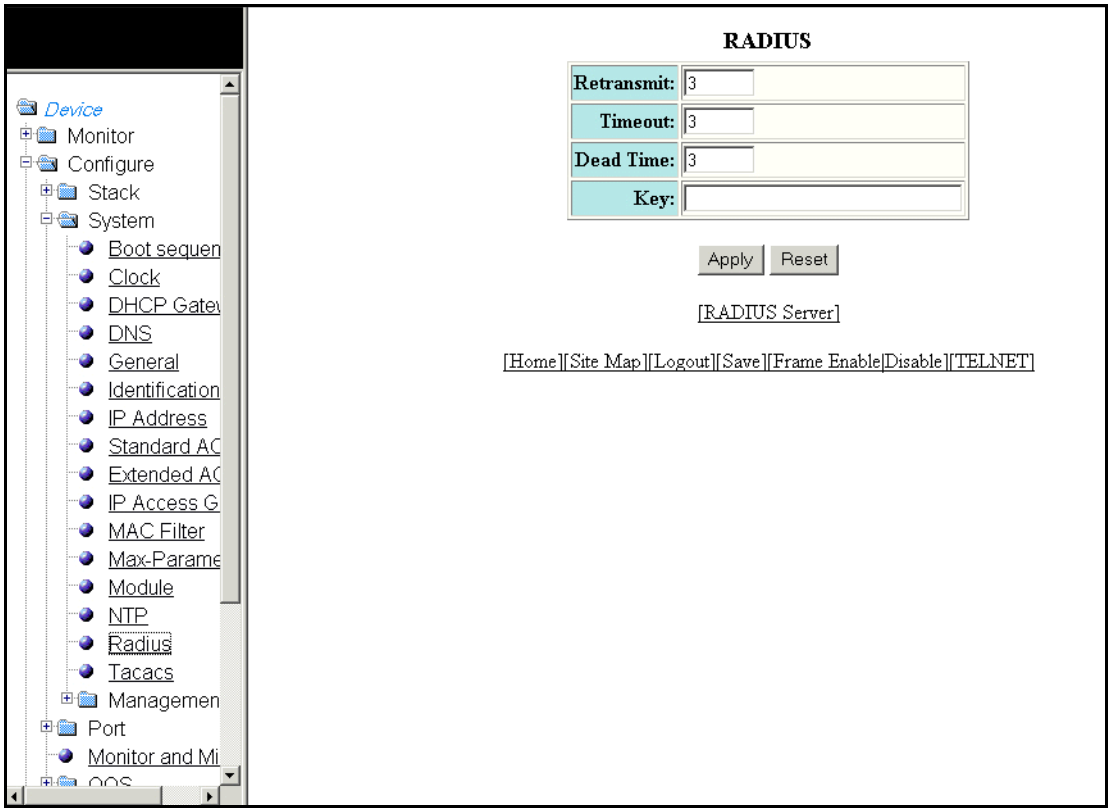
Configuring a RADIUS server

To configure a Remote Authentication Dial In User Service (RADIUS) server, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Radius**.

The **RADIUS** window is displayed as shown in Figure 91.

FIGURE 91 Configuring a RADIUS server



3. Type the retransmission interval, which specifies how many times the Brocade device resends an authentication request when the RADIUS server does not respond, in the **Retransmit** field. The range is from 1 through 5 times. The default is three times.
4. Type the timeout interval, which specifies how many seconds the Brocade device waits for a response from a RADIUS server before either retrying the authentication request or determining that the RADIUS servers are unavailable and moving on to the next authentication method in the authentication method list, in the **Timeout** field. The range is from 1 through 15 seconds. The default is three seconds.
5. Type the dead interval, which specifies how long the Brocade device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server, in the **Dead Time** field. The range is from 1 through 5 seconds. The default is three seconds.
6. Type the RADIUS key in the **Key** field. This is used to encrypt RADIUS packets before they are sent over the network. The value for the key parameter on the Brocade device should match the one configured on the RADIUS server. The key can be from 1 through 32 characters in length and cannot include any space characters.
7. Click **Apply**.

The message **The change has been made** is displayed. To display the configured RADIUS server, click **RADIUS Server**. To reset the data entered in the configuration pane, click **Reset**.

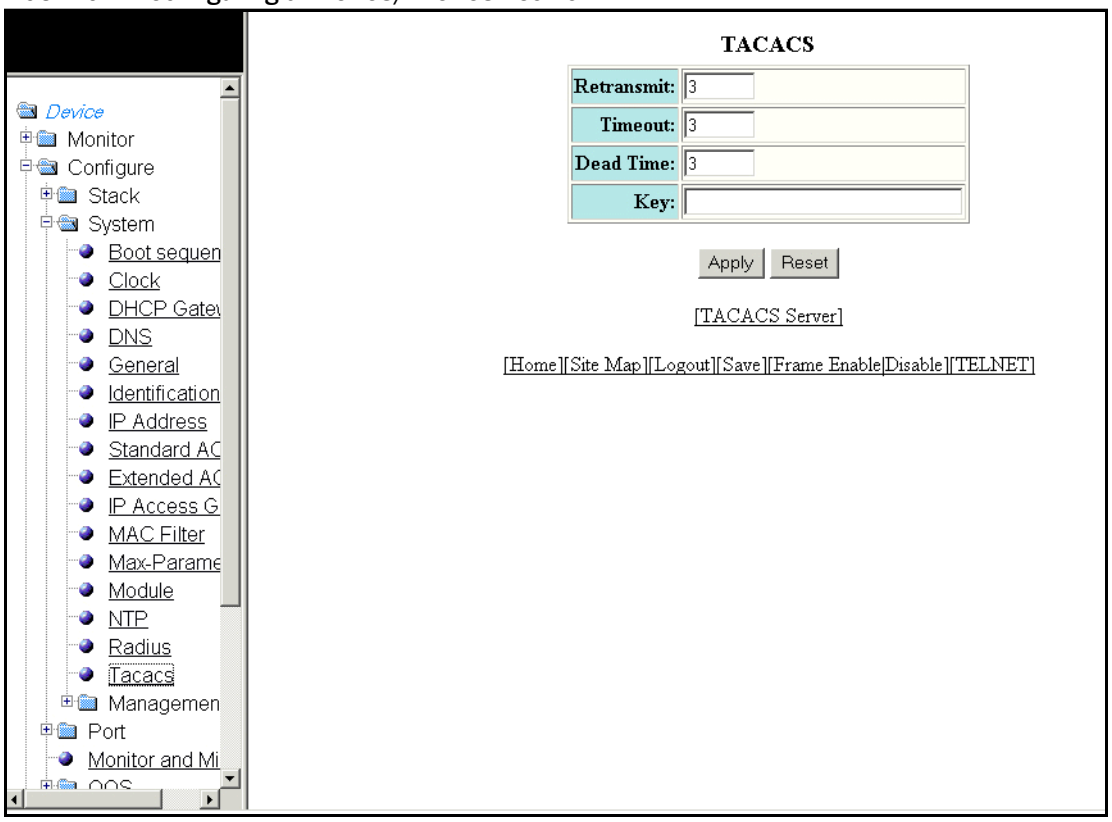
Configuring a TACACS/TACACS+ server

To configure a TACACS/TACACS+ server, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Tacacs**.

The **TACACS** window is displayed as shown in Figure 92.

FIGURE 92 Configuring a TACACS/TACACS+ server



3. Type the retransmission interval, which specifies how many times the Brocade device resends an authentication request when the TACACS/TACACS+ server does not respond, in the **Retransmit** field. The range is from 1 through 5 times. The default is three times.
4. Type the timeout interval, which specifies how many seconds the Brocade device waits for a response from a TACACS/TACACS+ server before either retrying the authentication request or determining that the TACACS/TACACS+ servers are unavailable and moving on to the next authentication method in the authentication method list, in the **Timeout** field. The range is from 1 through 15 seconds. The default is three seconds.
5. Type the dead interval, which specifies how long the Brocade device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server, in the **Dead Time** field. The range is from 1 through 5 seconds. The default is three seconds.

6. Type the TACACS/TACACS+ key in the **Key** field. This is used to encrypt TACACS/TACACS+ packets before they are sent over the network. The value for the key parameter on the Brocade device should match the one configured on the TACACS/TACACS+ server. The key can be from 1 through 32 characters in length and cannot include any space characters.
7. Click **Apply**.

The message **The change has been made** is displayed. To display the configured TACACS/TACACS+ server, click **TACACS Server**. To reset the data entered in the configuration pane, click **Reset**.

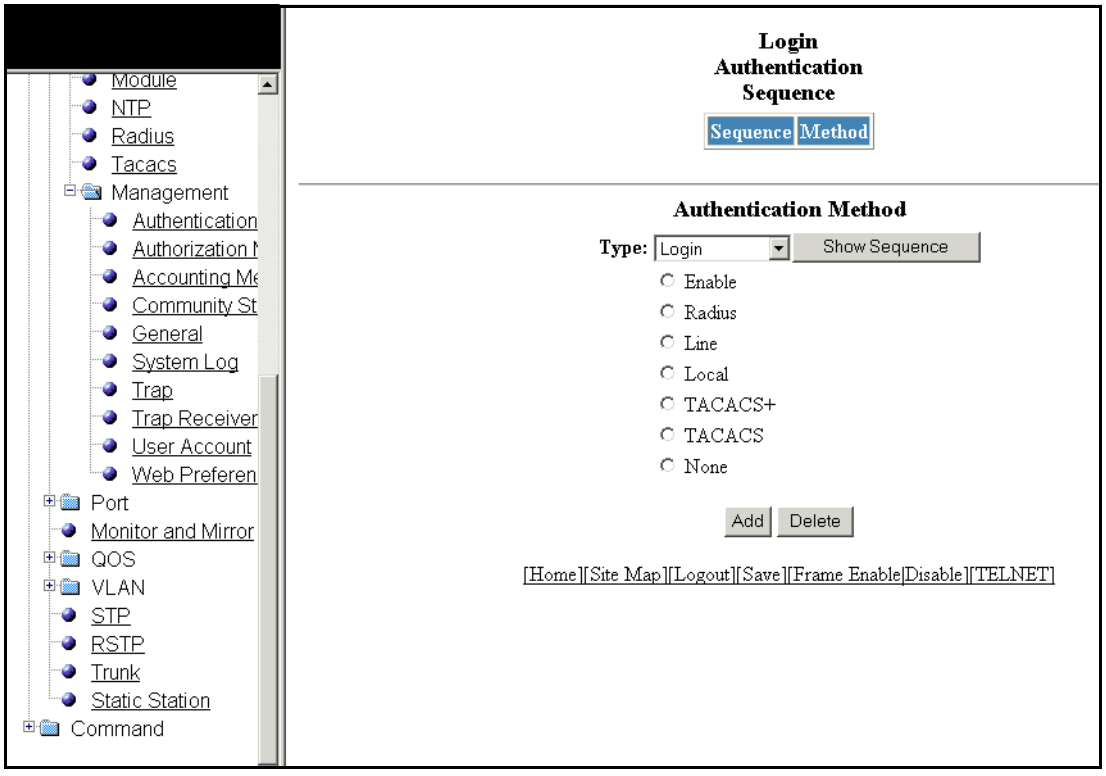
Configuring management authentication

To configure management authentication, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Authentication Methods**.

The **Authentication Method** window is displayed as shown in Figure 93.

FIGURE 93 Configuring management authentication



3. Select one of the following types of authentication in the **Type** list:
   - **Login**
   - **Enable**
   - **Web Server**
   - **SNMP Server**

4. Click one of the following servers:
   - **Enable**
   - **Radius**
   - **Line**
   - **Local**
   - **TACACS+**
   - **TACACS**
   - **None**
5. Click **Add**.

The message **The change has been made** is displayed and the configured authentication method is listed in the **Login Authentication Sequence** pane. Click **Show Sequence** to display the list of authentication methods added. To remove the configured management authentication, click **Delete.**

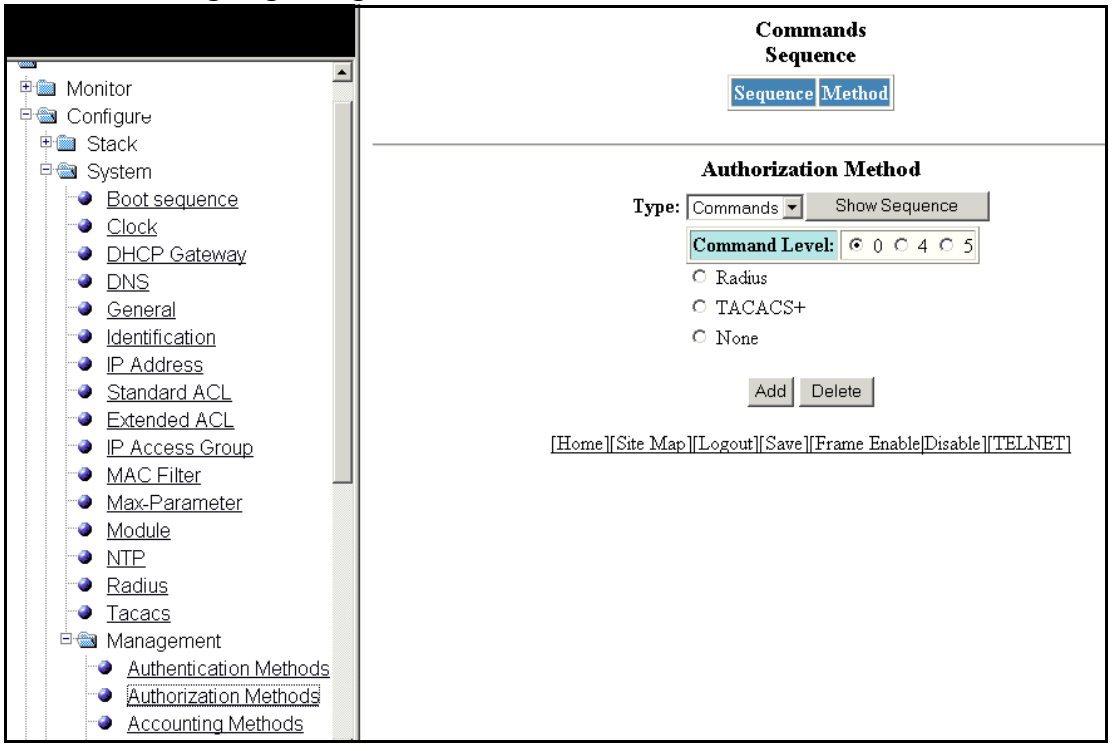
Configuring management authorization

To configure management authorization, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Authorization Methods**.

The **Authorization Method** window is displayed as shown in Figure 94.

FIGURE 94 Configuring management authorization



3. Select either of the following modes of authorization in the **Type** list:
   - **Commands**
   - **Exec**
4. Click **0** or **4** or **5** for **Command Level**.
5. Click one of the following servers:
   - **Radius**
   - **TACACS+**
   - **None**
6. Click **Add**.

The message **The change has been made** is displayed and the configured authorization method is listed in the **Commands Sequence** pane. Click **Show Sequence** to display the list of authentication methods added. To delete the configured management authorization, click **Delete**.

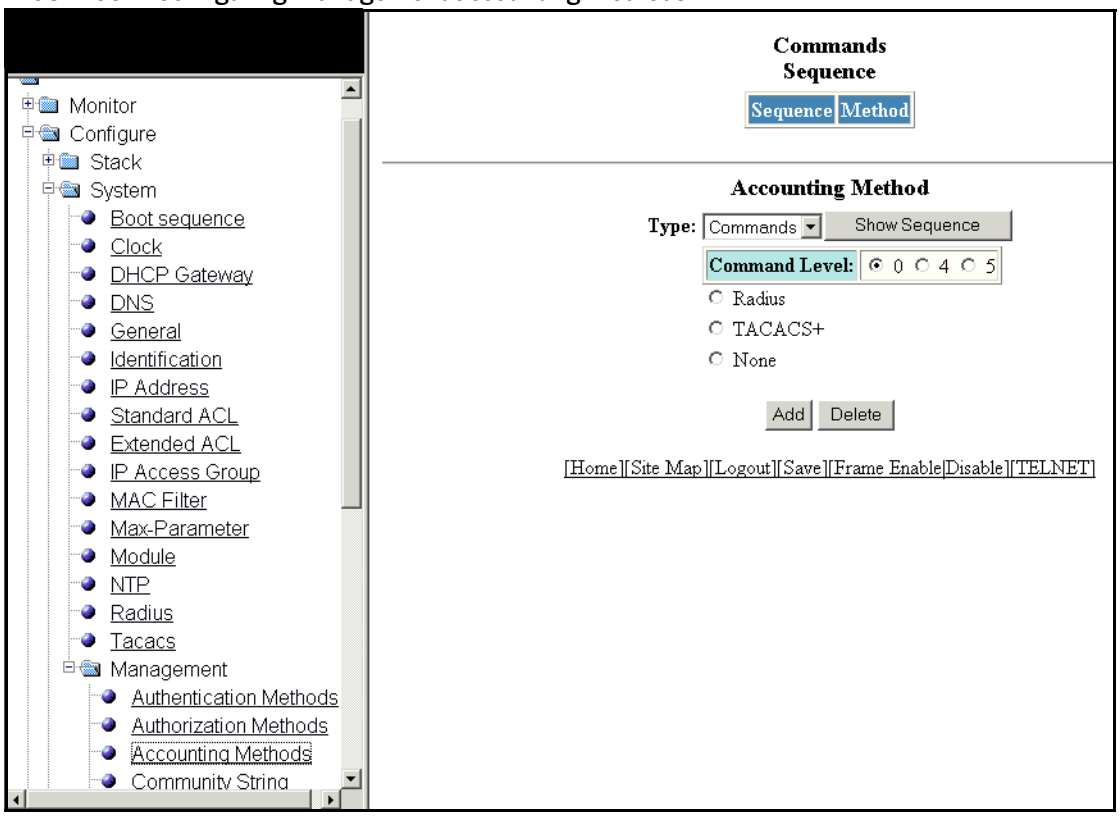
Configuring management accounting

To configure management accounting, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Accounting Methods.**

The **Accounting Method** window is displayed as shown in Figure 95.

FIGURE 95 Configuring management accounting methods



3. Select one of the following modes of authorization:
   - **Commands**
   - **Exec**
   - **System**
4. Click **0** or **4** or **5** for **Command Level**.
5. Click one of the following servers:
   - **Radius**
   - **TACACS+**
   - **None**
6. Click **Add**.

The message **The change has been made** is displayed and the configured accounting method is listed in the **Commands Sequence** pane. To delete the configured accounting method, click **Delete**.

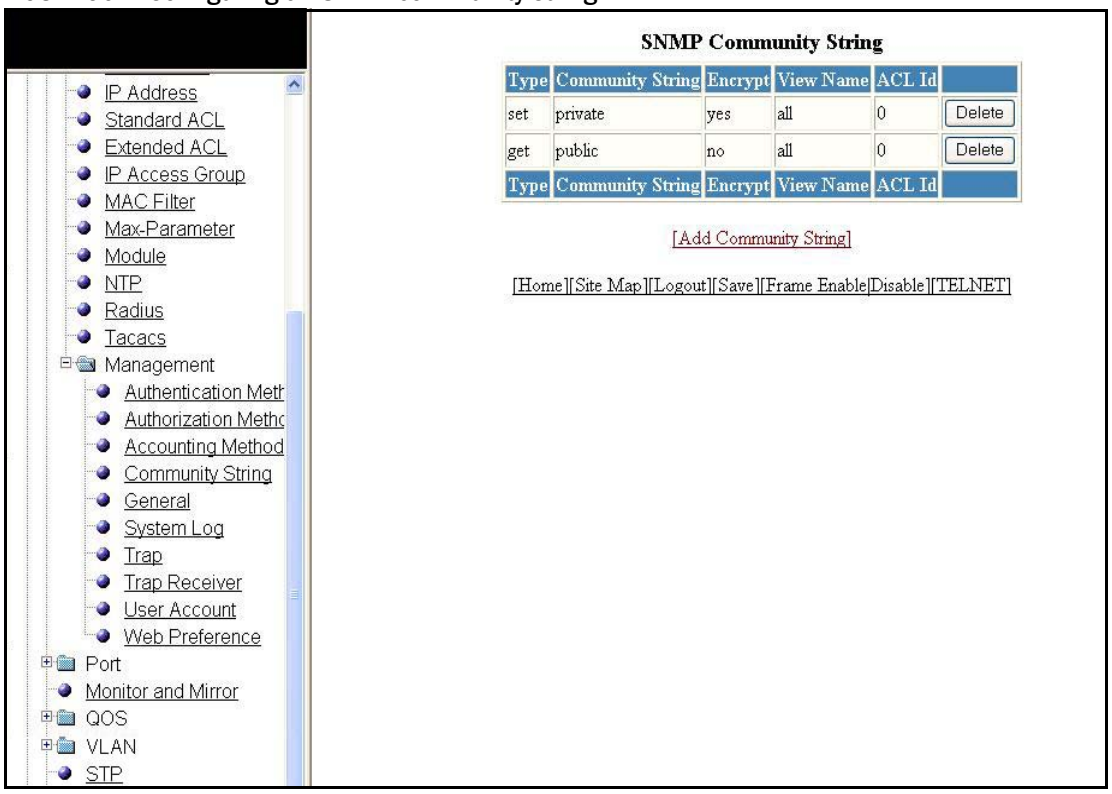
Configuring an SNMP community string

To configure an SNMP community string, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Community String.**

The **SNMP Community String** window is displayed as shown in Figure 96.

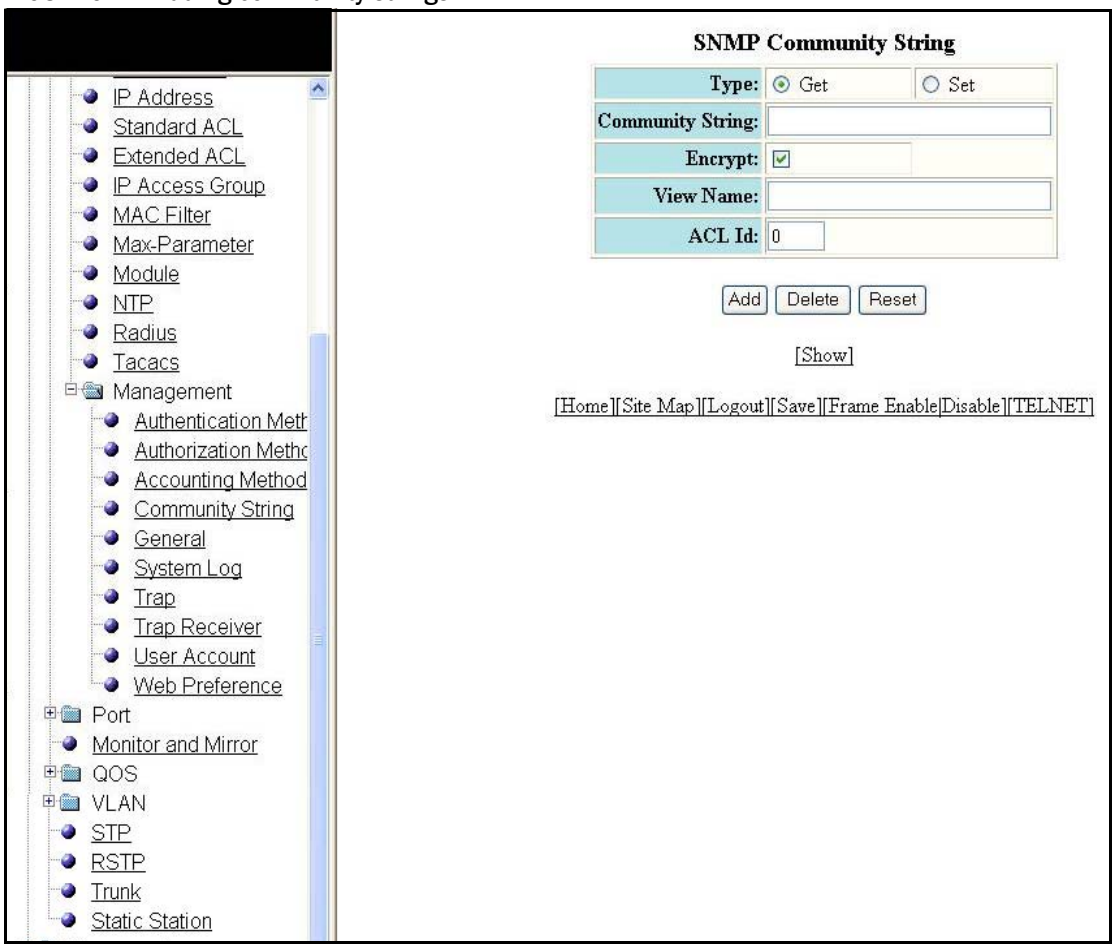
FIGURE 96 Configuring an SNMP community string



3. Click **Add Community String**.

The **SNMP Community String** window is displayed as shown in Figure 97.

FIGURE 97 Adding community strings



4. Click **Get** or **Set** for **Type**.
5. Type the user name to open a web management session in the **Community String** field.
6. Select the **Encrypt** check box to enable encryption for a particular string.
7. Type the name of the community string in the **View Name** field.
8. Type the ACL number in the **ACL Id** field.
9. Click **Add**.

The message **The change has been made** is displayed. To display the configured community string, click **Show**.

To delete the community string, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

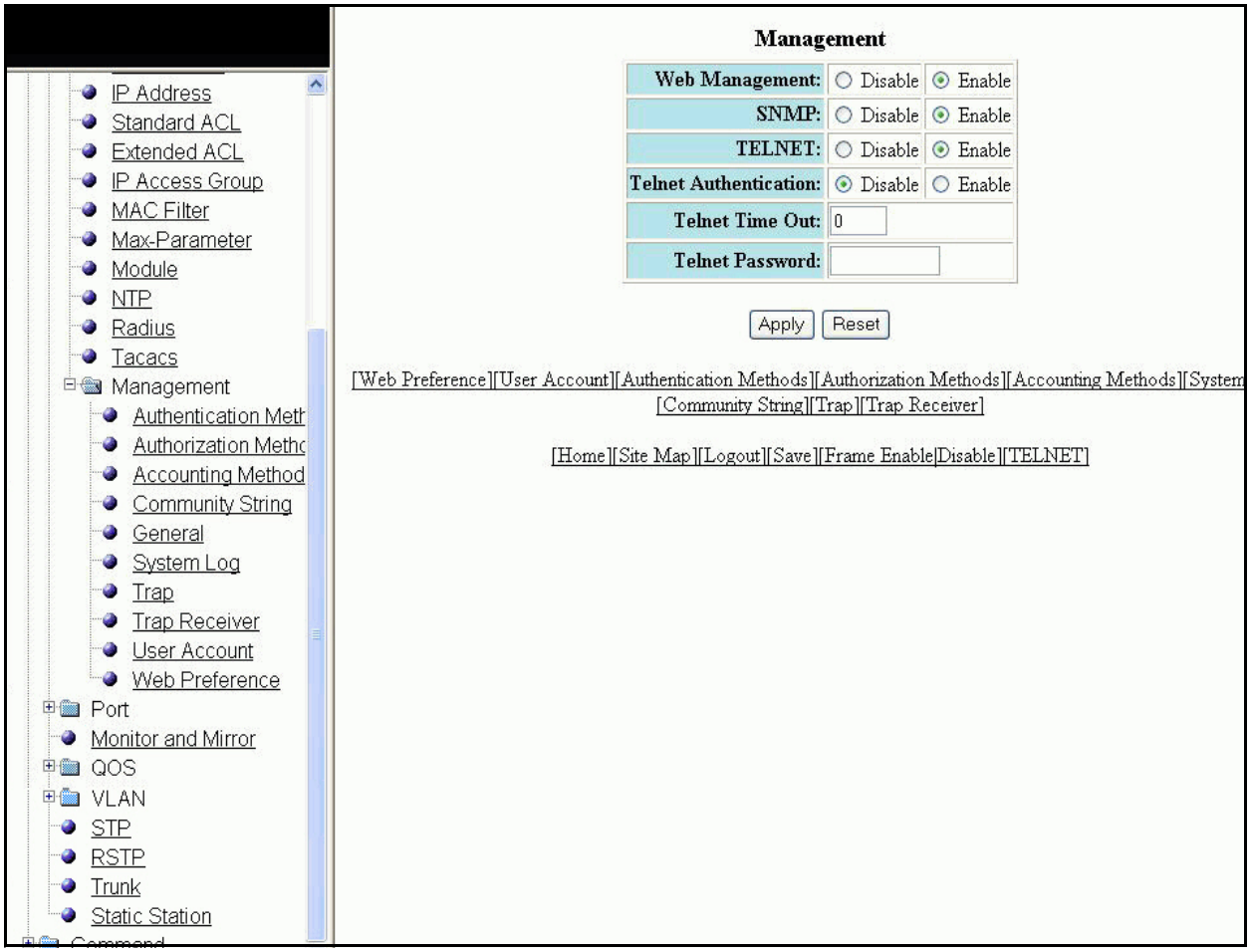
Configuring the general management parameters

To configure the general management parameters, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **General**.

The **Management** window is displayed as shown in Figure 98.

FIGURE 98 Configuring general management parameters



3. Select **Disable** or **Enable** for **Web Management**.
4. Select **Disable** or **Enable** for **SNMP**.
5. Select **Disable** or **Enable** for **TELNET**.
6. Select **Disable** or **Enable** for **Telnet Authentication**.
7. Type the timeout interval in seconds to wait for a response in the **Telnet Time Out** field.
8. Type an alphanumeric password in the **Telnet Password** field.
9. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

The **Management** window provides links to configure other management parameters:

- To configure the web management preferences, click **Web Preference**. For more information, refer to "Configuring the web management preference" on page 169.
- To configure a management user account, click **User Account**. For more information, refer to "Configuring a management user account" on page 168.
- To configure management authentication, click **Authentication Methods**. For more information, refer to "Configuring management authentication" on page 155.
- To configure management authorization, click **Authorization Methods**. For more information, refer to "Configuring management authorization" on page 156.
- To configure management accounting, click **Accounting Methods**. For more information, refer to "Configuring management accounting" on page 157.
- To configure a system module, click **System**. For more information, refer to "Configuring a system module" on page 149.
- To configure an SNMP community string, click **Community String**. For more information, refer to "Configuring a system module" on page 149.

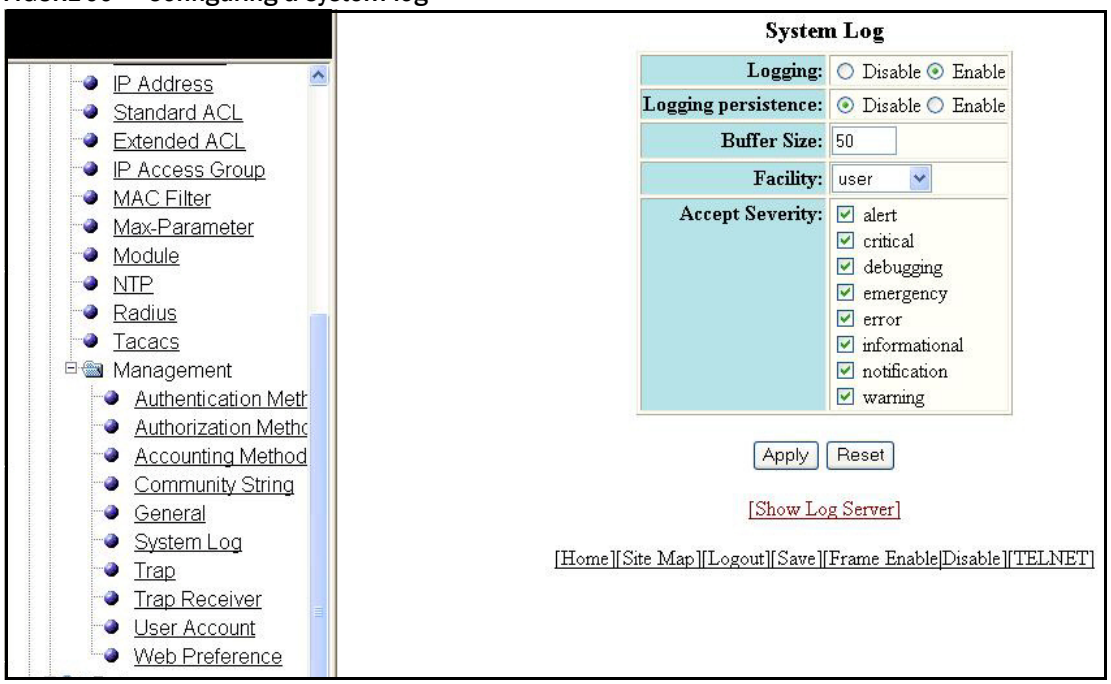
Configuring a management system log

To configure a management system log, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **System Log**.

The **System Log** window is displayed as shown in Figure 99.

FIGURE 99 Configuring a system log

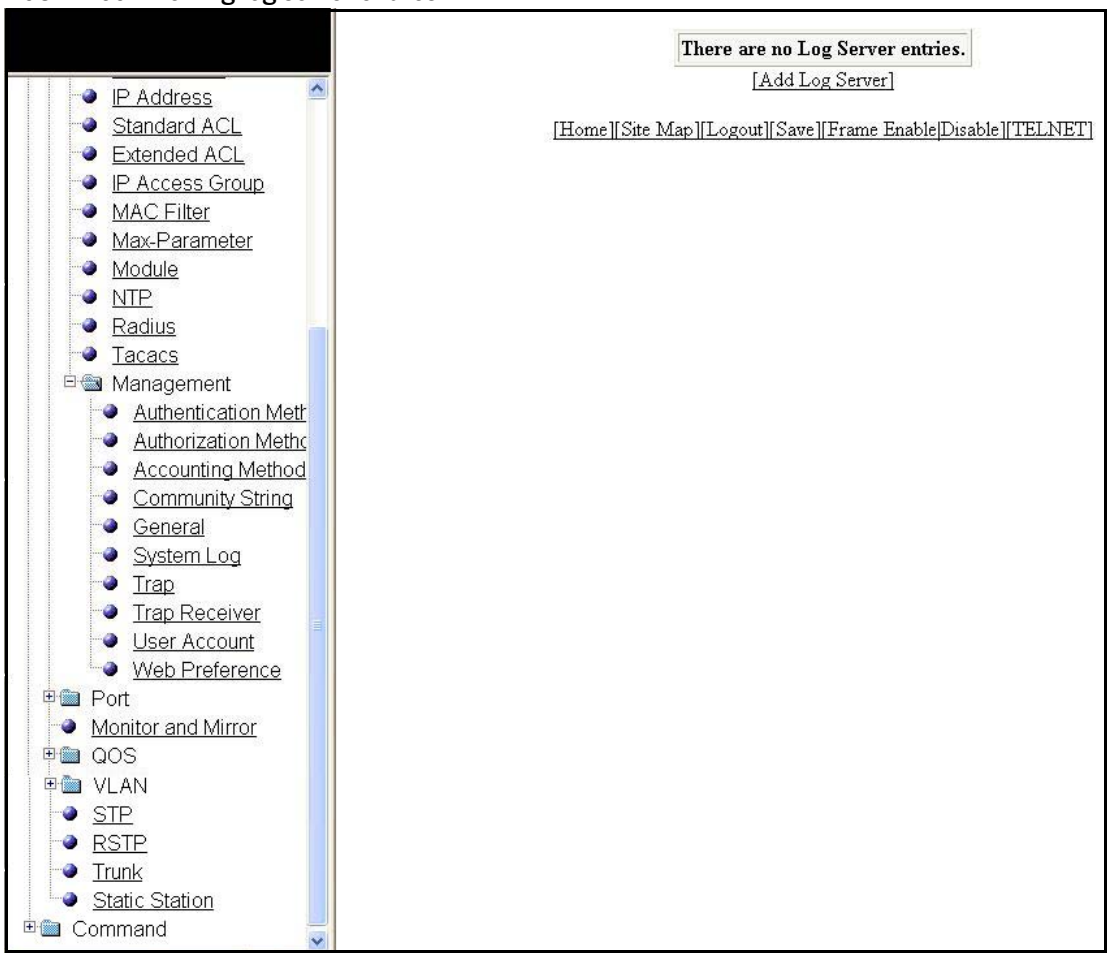


3. Click **Disable** or **Enable** for **Logging**. By default, the syslog buffer is enabled.
4. Click **Disable** or **Enable** for **Logging persistence**. By default, logging persistence is disabled.
5. Type the number of messages in the **Buffer Size** field.
6. Select a facility in the **Facility** list.
7. Select one of the following severity levels for **Accept Severity**:
   - **alert**
   - **critical**
   - **debugging**
   - **emergency**
   - **error**
   - **informational**
   - **notification**
   - **warning**
8. Click **Apply**.

The message **The change has been made** is displayed. To display log server entries, click **Show Log Server**. To reset the data entered in the configuration pane, click **Reset**.

If there are no log servers, the message **There are no Log Server entries** is displayed as shown in Figure 100.

FIGURE 100 Viewing log server entries

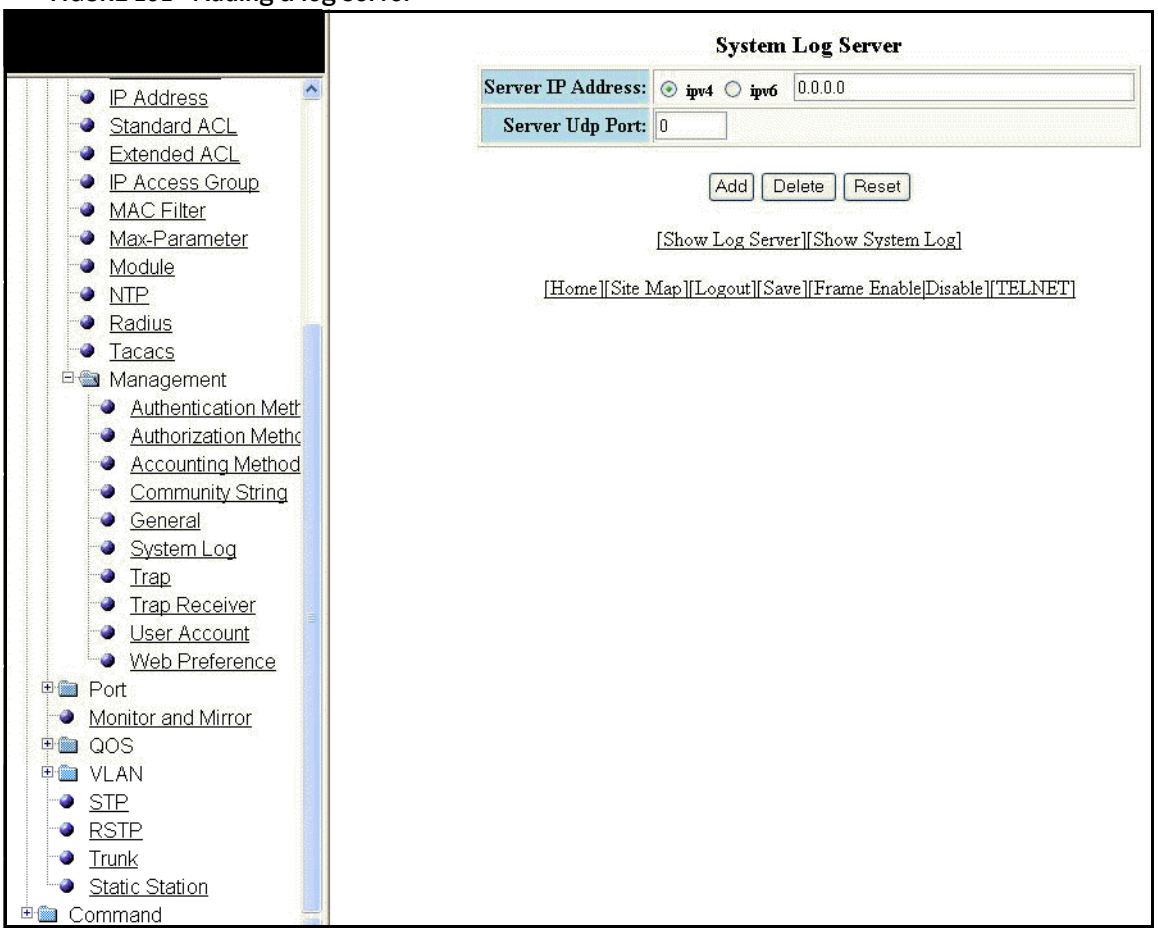


To add extra log servers to your system log configuration, perform the following steps.

1. Click **Add Log Server**.

The **System Log Server** window is displayed as shown in Figure 101.

FIGURE 101 Adding a log server



2. Click **ipv4** or **ipv6** and then type the IPv4 or IPv6 address in the **Server IP Address** field.
3. Type the application port that can be used for the syslog facility in the **Server Udp Port** field. The default value is 514.
4. Click **Add**.

The message **The change has been made** is displayed. To display the log server entries, click **Show Log Server**. To display the system log window, click **Show System Log**.

To delete the changes made, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

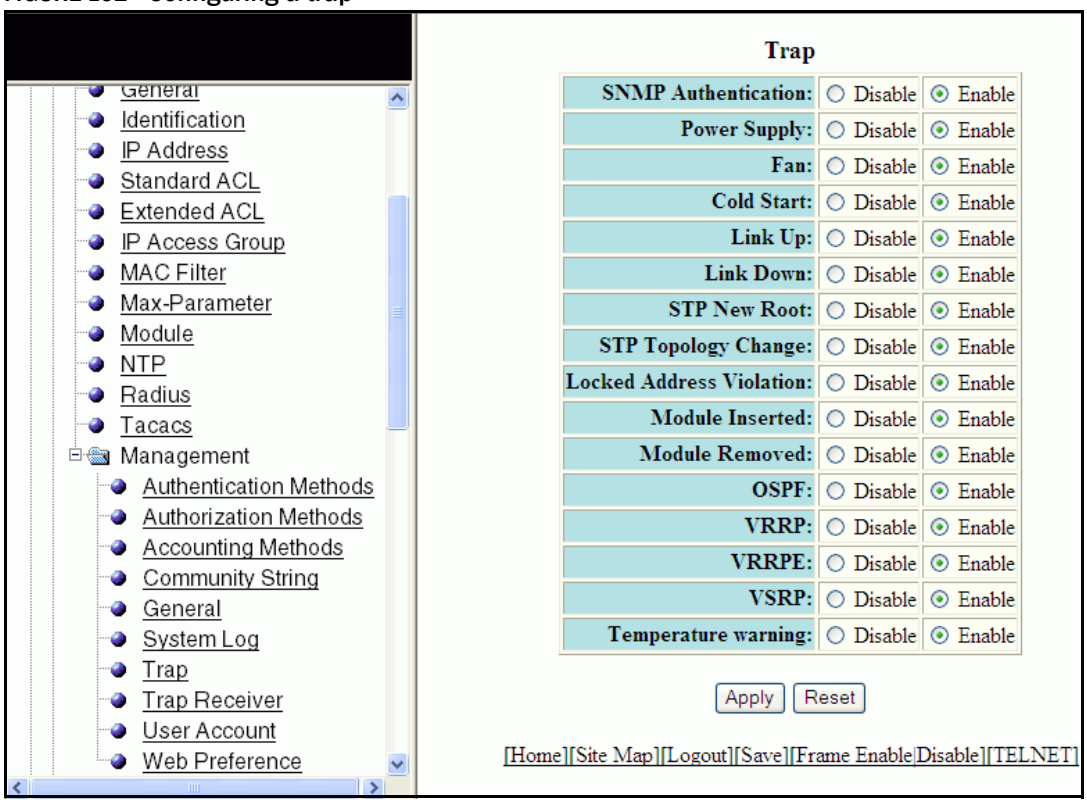
Configuring a trap

To configure a trap, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Trap**.

The **Trap** window is displayed as shown in Figure 102.

FIGURE 102 Configuring a trap



3. Click **Disable** or **Enable** for **SNMP Authentication**.
4. Click **Disable** or **Enable** for **Power Supply**.
5. Click **Disable** or **Enable** for **Fan**.
6. Click **Disable** or **Enable** for **Cold Start**.
7. Click **Disable** or **Enable** for **Link Up**.
8. Click **Disable** or **Enable** for **Link Down**.
9. Click **Disable** or **Enable** for **STP New Root**.
10. Click **Disable** or **Enable** for **STP Topology Change**.
11. Click **Disable** or **Enable** for **Locked Address Violation**.
12. Click **Disable** or **Enable** for **Module Inserted**.
13. Click **Disable** or **Enable** for **Module Removed**.
14. Click **Disable** or **Enable** for **OSPF**.
15. Click **Disable** or **Enable** for **VRRP**.
16. Click **Disable** or **Enable** for **VRRPE**.
17. Click **Disable** or **Enable** for **VSRP**.
18. Click **Disable** or **Enable** for **Temperature warning**.
19. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

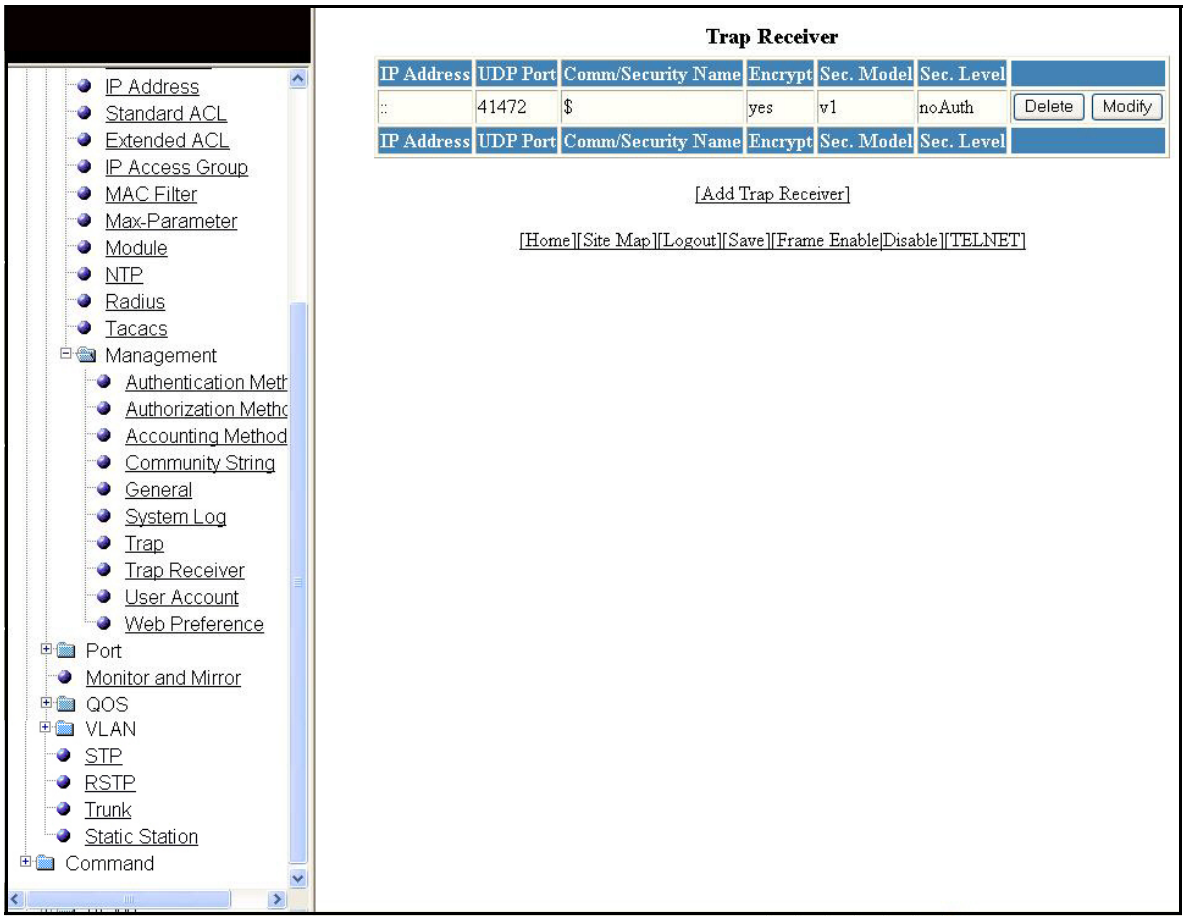
Configuring a trap receiver

To configure a trap receiver, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Trap Receiver**.

The **Trap Receiver** window is displayed as shown in Figure 103.

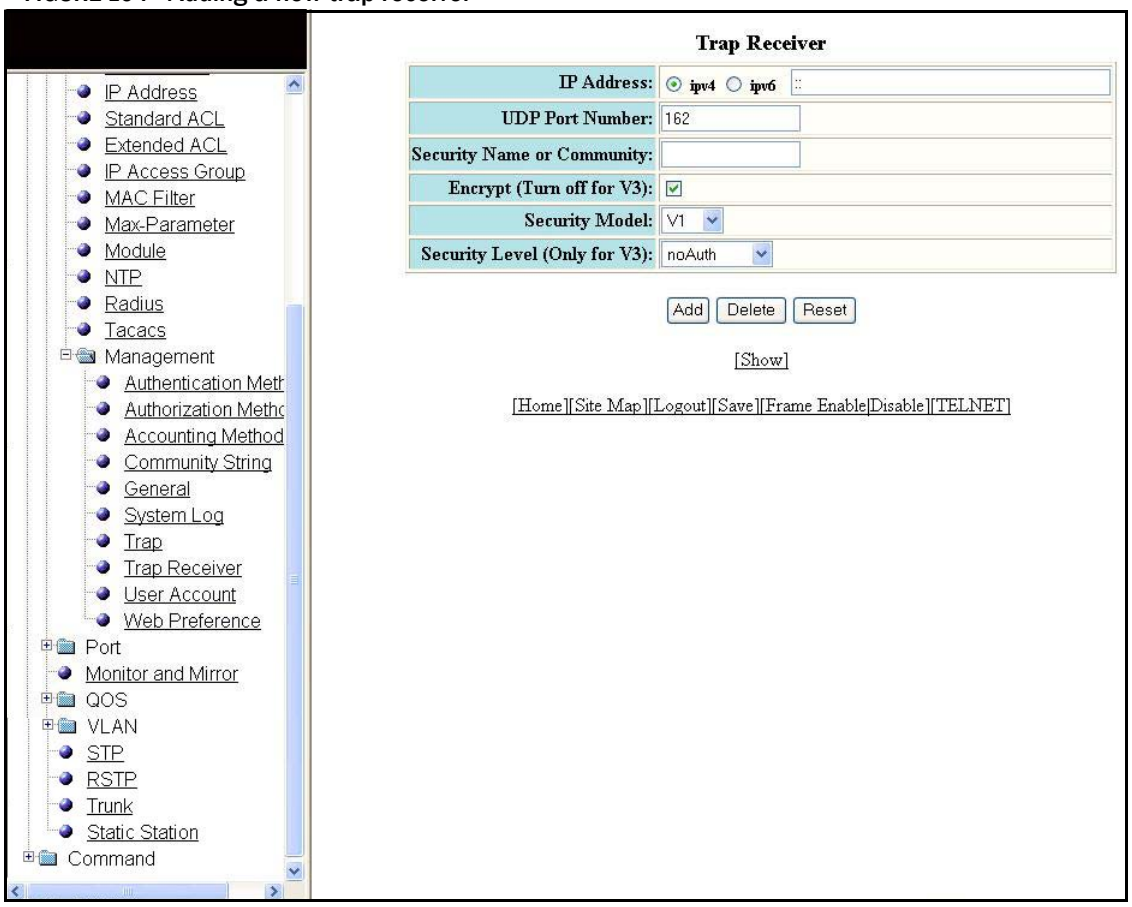
FIGURE 103 Configuring a trap receiver



3. Click **Add Trap Receiver** to configure a new trap receiver.

The **Trap Receiver** window is displayed as shown in Figure 104.

FIGURE 104 Adding a new trap receiver



4. Click **ipv4** or **ipv6** and then type the IP address of the destination of the route in the **IP Address** field.
5. Type the UDP port number of the host that will receive the trap in the **UDP Port Number** field.
6. Type an arbitrary value made of two five-digit integers joined by a colon in the **Security Name or Community** field. Each string in the community name can be a number from 0 through 65535.
7. Select the **Encrypt (Turn off for V3)** check box to enable or disable encryption for a particular string. It is turned off for V3.
8. Select one of the following options in the **Security Model** list:
   - **V1**
   - **V2C**
   - **V3**
9. For V3 only, select one of the following options in the **Security Level (Only for V3)** list:
   - **noAuth** - Allow all packets.
   - **authNoPriv** - Allow only authenticated packets.
   - **authPriv** - A password is required.
10. Click **Add**.

The message **The change has been made** is displayed. To view the trap receiver entries, click **Show**.

To delete the trap receiver, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

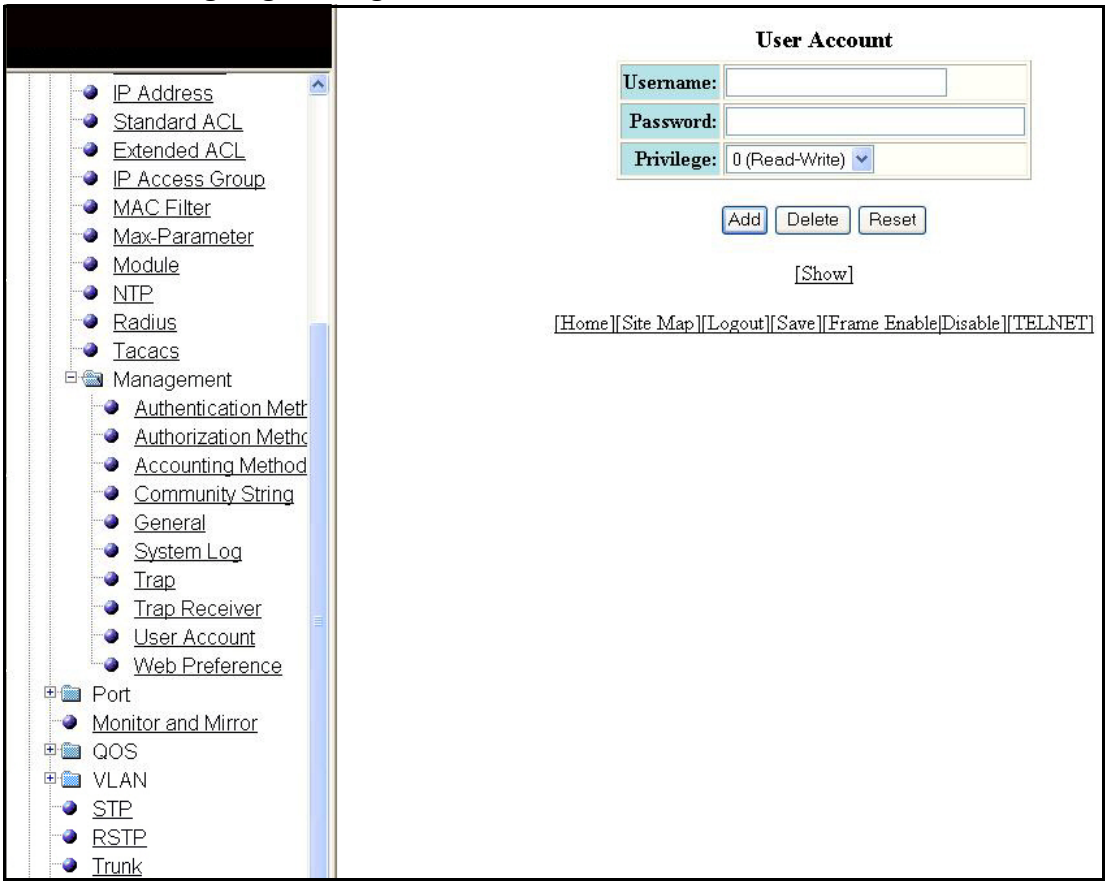
Configuring a management user account

To configure a management user account, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **User Account**.

The **User Account** window is displayed as shown in Figure 105.

FIGURE 105 Configuring a management user account



3. Type the user identifier in the **Username** field.
4. Type the login password in the **Password** field.
5. Select one of the following options in the **Privilege** list:
   - **0 (Read-Write)**
   - **4 (Port-Config)**
   - **5 (Read-Only)**
6. Click **Add**.

The message **The change has been made** is displayed. To view the configured user account, click **Show**.

To delete the configured user account, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

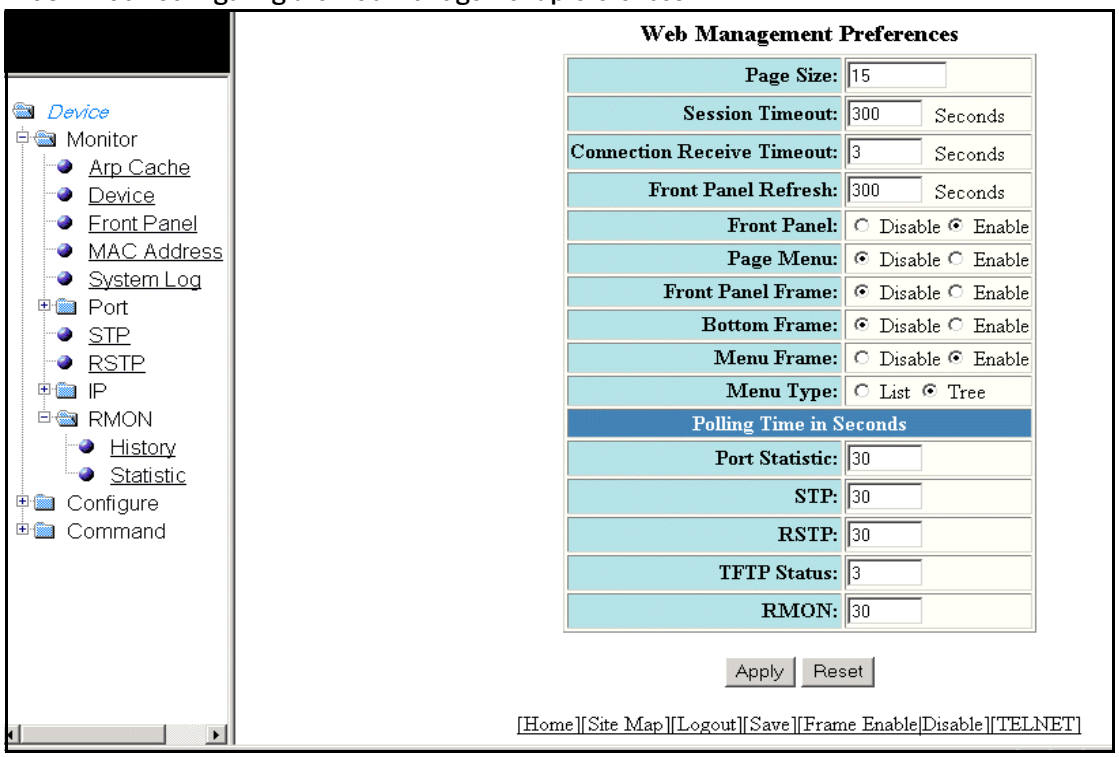
Configuring the web management preference

To configure the web management preferences, perform the following steps.

1. Click **Configure** on the left pane and select **System**.
2. Click **Management** and select **Web Preference**.

The **Web Management Preference** window for Brocade FSX devices is displayed as shown in Figure 106.

FIGURE 106 Configuring the web management preferences



3. Type the page size in the **Page Size** field.
4. Type the console session timeout value in seconds in the **Session Timeout** field.
5. Type the wait time interval after getting disconnected from the application in the **Connection Receive Timeout** field.
6. Type the number of seconds after which the front panel gets refreshed in the **Front Panel Refresh** field.
7. Click **Disable** or **Enable** for **Front Panel**. By default, it is enabled and the ports are labelled on the front panel of the devices.

8. Click **Disable** or **Enable** for **Page Menu**.
9. Click **Disable** or **Enable** for **Front Panel Frame**.
10. Click **Disable** or **Enable** for **Bottom Frame**.
11. Click **Disable** or **Enable** for **Menu Frame**.
12. Click **List** or **Tree** for **Menu Type**.
13. Type the port statistics polling time in the **Port Statistic** field.
14. Type the STP statistics polling time in the **STP** field.
15. Type the RSTP statistics polling time in the **RSTP** field.

NOTE
The **RSTP** field is not available in the **Web Management Preference** window for Brocade FCX and Brocade ICX 6610 devices.

16. Type the TFTP polling time in seconds in the **TFTP Status** field.
17. Type the polling time for Remote Monitoring in the **RMON** field.
18. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

Chapter

16

Configuring Module Components

In this chapter

- Configuring a module 171
- Modifying inline power budget 172

NOTE
This chapter is specific to Brocade FSX devices.

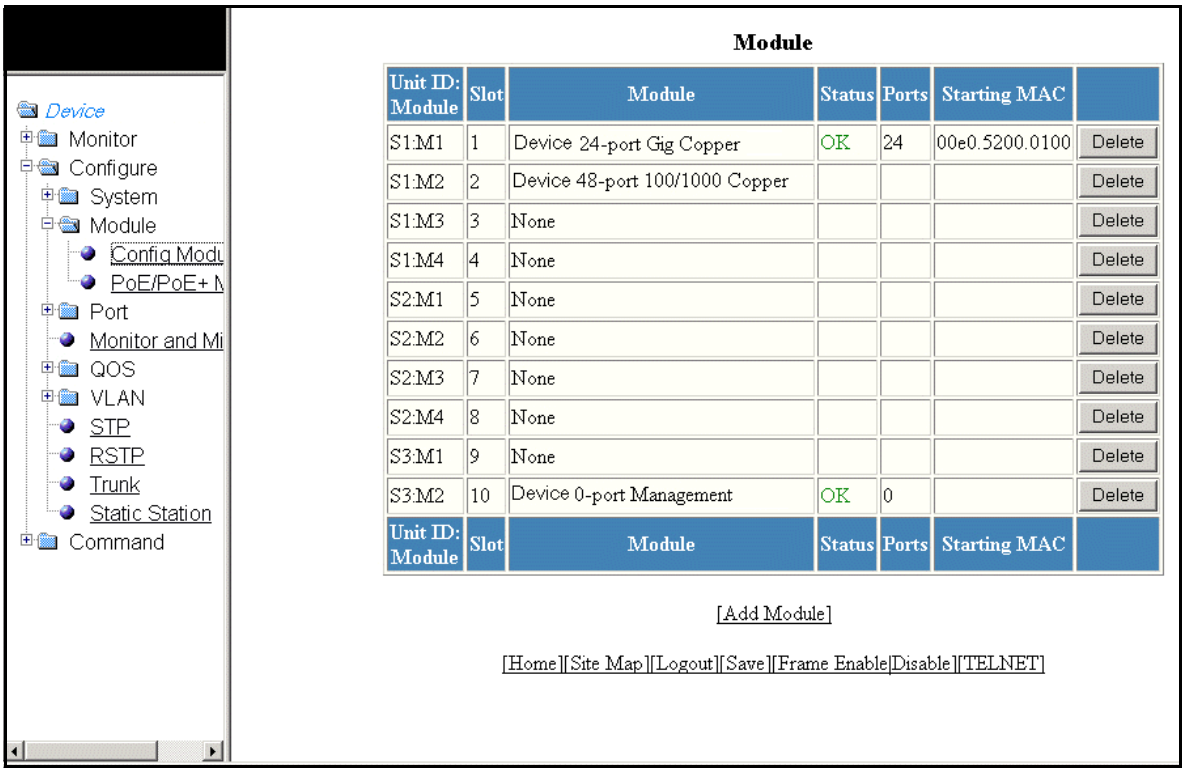
Configuring a module

To configure a chassis module, perform the following steps.

1. Click **Configure** on the left pane and select **Module**.
2. Click **Config Module**.

The **Module** window is displayed as shown in Figure 107.

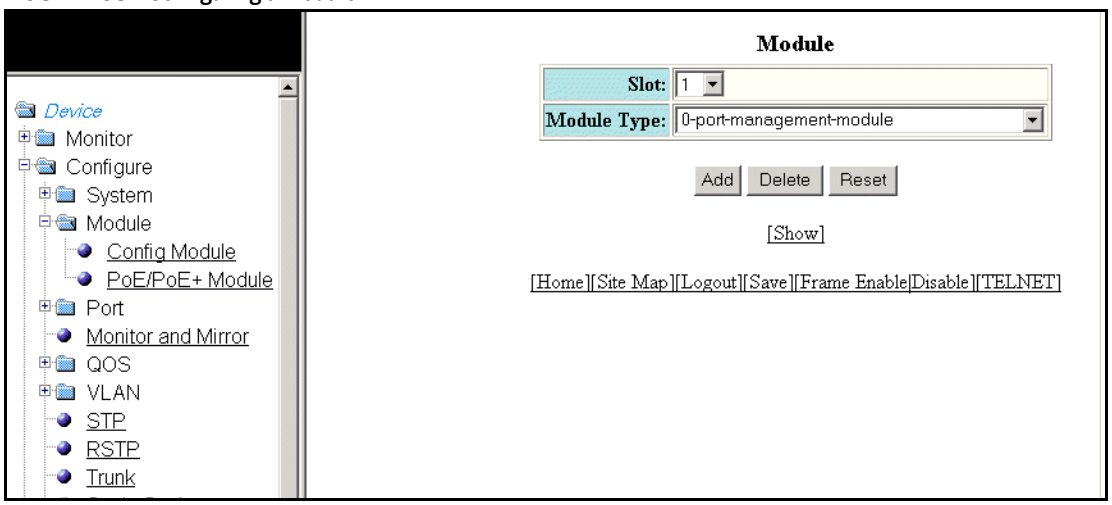
FIGURE 107 Configuring a module



3. Click **Add Module**.

The **Module** window is displayed as shown in Figure 108.

FIGURE 108 Configuring a module



4. Select a slot number in the **Slot** list.
5. Select a chassis module type in the **Module Type** list.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured module, click **Show**.

To delete the configured module, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

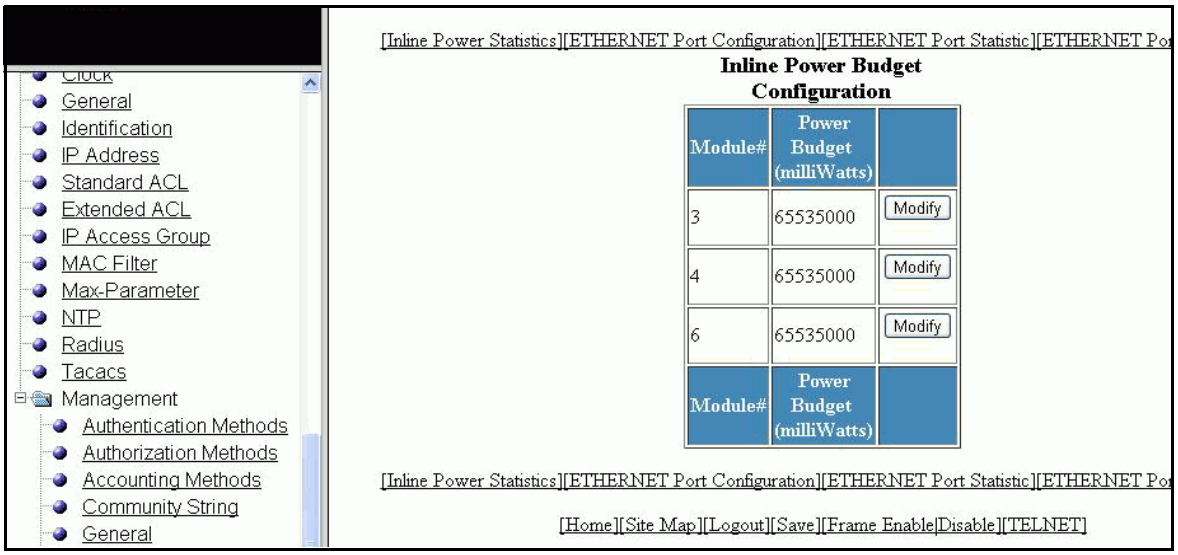
Modifying inline power budget

To configure Power over Ethernet (PoE), perform the following steps.

1. Click **Configure** on the left pane and select **Module**.
2. Click **PoE/PoE+ Module**.

The **Inline Power Budget Configuration** window is displayed as shown in Figure 109.

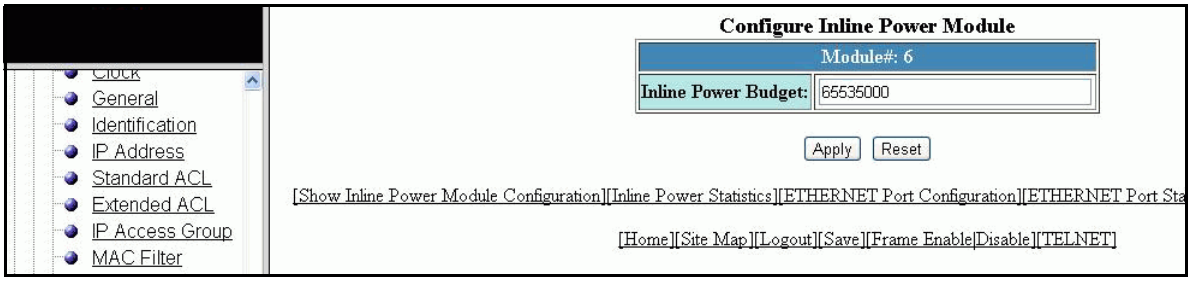
FIGURE 109 Configuring PoE



3. Click **Modify**.

The **Configure Inline Power Module** window is displayed as shown in Figure 110.

FIGURE 110 Modifying the inline power module



4. Type the number of milliwatts (from 0 through 65535000) to allocate to the module in the **Inline Power Budget** field. The default value is 65535000 milliwatts.
5. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**. To display the configured inline power budget, click **Show Inline Power Module Configuration**.

The **Inline Power Budget Configuration** window provides links to monitor the power budget of the PoE or PoE+ modules and to configure and monitor port parameters:

- To display the power budget of the PoE or PoE+ module, click **Inline Power Statistics**. For more information, refer to "Displaying inline power details" on page 47.
- To configure an Ethernet port, click **Ethernet Port Configuration**. For more information, refer to "Configuring an Ethernet port" on page 175.

- To view the total number of packets, number of collisions, and number of errors that have occurred on a port, click **Ethernet Port Statistic**. For more information, refer to "Displaying Ethernet port statistics" on page 35.
- To view the traffic that is received and transmitted on a port, click **Ethernet Port Utilization**. For more information, refer to "Displaying Ethernet port utilization" on page 39.

Chapter

17

Configuring Port Parameters

In this chapter

- Configuring an Ethernet port 175
- Configuring port inline power 177
- Configuring a management port 178
- Configuring the port uplink relative utilization 179

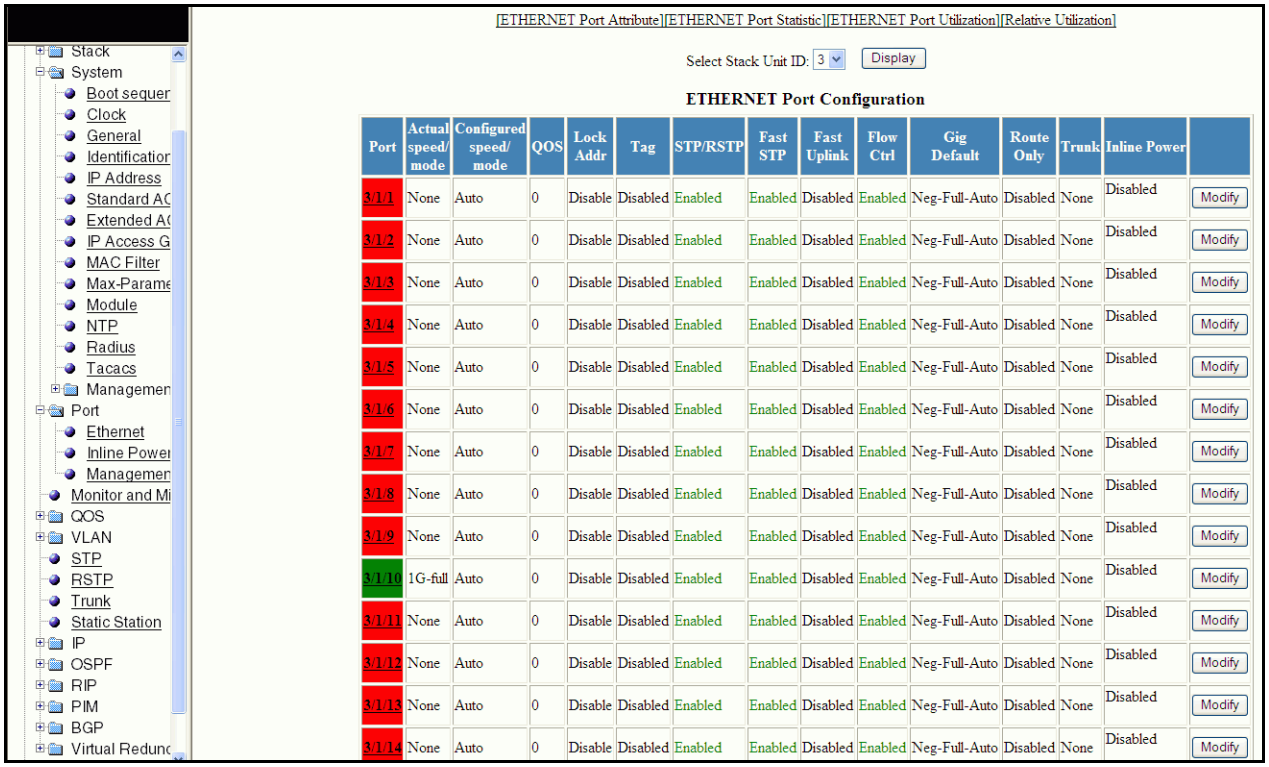
Configuring an Ethernet port

To configure an Ethernet port, perform the following steps.

1. Click **Configure** on the left pane and select **Port**.
2. Click **Ethernet**.

The **ETHERNET Port Configuration** window is displayed as shown in Figure 111.

FIGURE 111 Configuring an Ethernet port



Port	Actual speed/ mode	Configured speed/ mode	QOS	Lock Addr	Tag	STP/RSTP	Fast STP	Fast Uplink	Flow Ctrl	Gig Default	Route Only	Trunk	Inline Power	
3/1/1	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/2	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/3	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/4	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/5	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/6	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/7	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/8	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/9	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/10	1G-full	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/11	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/12	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/13	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify
3/1/14	None	Auto	0	Disable	Disabled	Enabled	Enabled	Disabled	Enabled	Neg-Full-Auto	Disabled	None	Disabled	Modify

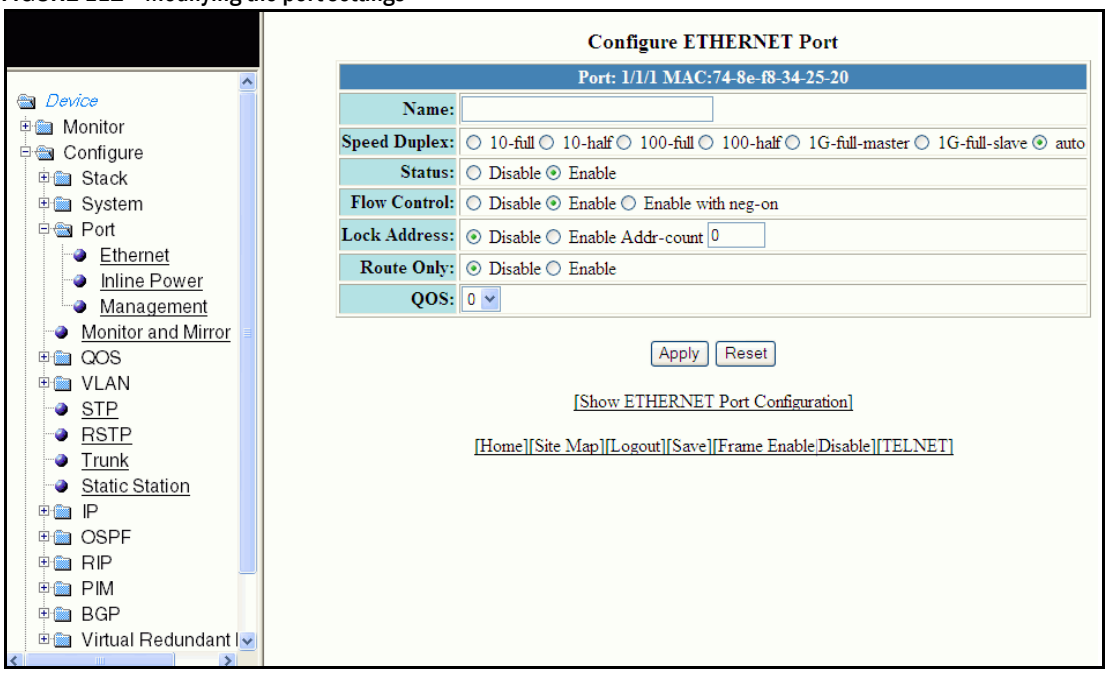
3. For Brocade FCX and Brocade ICX 6610 devices, select a unit ID in the **Select Stack Unit ID** list and click **Display** to display the information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available in the **ETHERNET Port Configuration** window for Brocade FSX devices.

4. Click **Modify** to modify the respective Ethernet port.

The **Configure ETHERNET Port** window is displayed as shown in Figure 112.

FIGURE 112 Modifying the port settings



5. Type the name of the Ethernet port in the **Name** field.
6. Select the type of the port speed for **Speed Duplex**, which can be one of the following:
   - **10-full** – 10 Mbps, full duplex
   - **10-half** – 10 Mbps, half duplex
   - **100-full** – 100 Mbps, full duplex
   - **100-half** – 100 Mbps, half duplex
   - **1G-full-master** – 1 Gbps, full duplex master
   - **1G-full-slave** – 1 Gbps, full duplex slave
   - **auto** – Auto-negotiation
7. Click **Disable** or **Enable** for **Status** to disable or enable an Ethernet port.
8. Click **Disable** or **Enable** or **Enable with neg-on** for **Flow Control**. By default, flow control is enabled.
9. Click **Disable** or **Enable** for **Lock Address**. If you click **Enable**, type the number of devices that can have access to a specific port in the **Addr-count** field.

10. Click **Disable** or **Enable** for **Route Only**. If you click **Enable**, Layer 2 switching is disabled globally.
11. Select the QoS priority for the port in the **QOS** list.
12. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

To display the **ETHERNET Port Configuration** window, click **Show ETHERNET Port Configuration**.

To display the inline power statistics for a PoE stack device, click **Show Inline Power**. For more information, refer to "Displaying port inline power for Brocade FCX and Brocade ICX 6610 devices" on page 44.

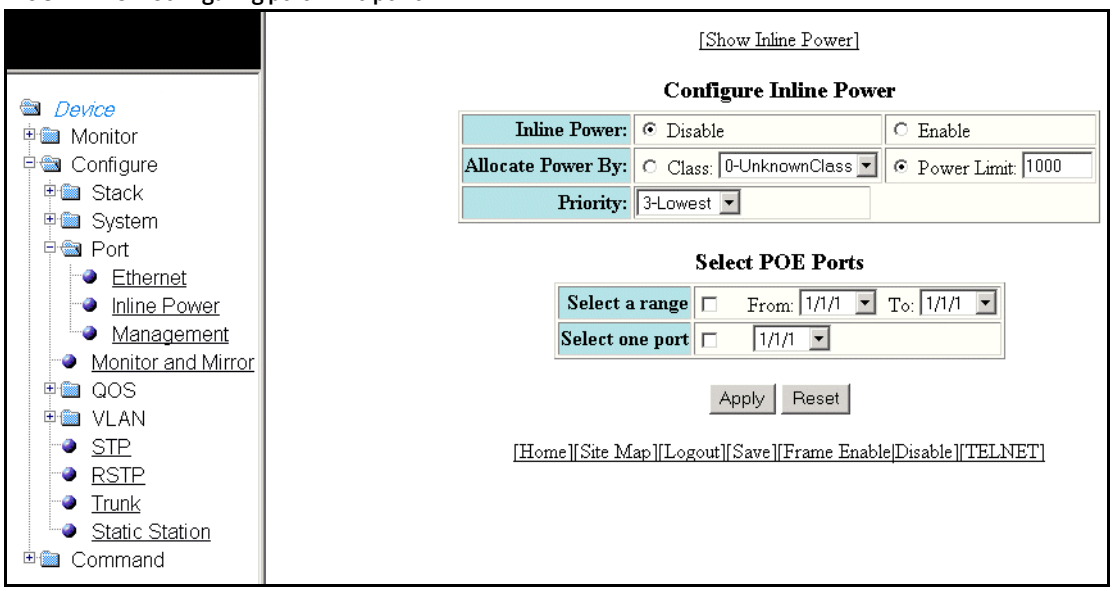
Configuring port inline power

To configure port inline power, perform the following steps.

1. Click **Configure** on the left pane and select **Port**.
2. Click **Inline Power**.

The **Configure Inline Power** window is displayed as shown in Figure 113.

FIGURE 113 Configuring port inline power



3. Click **Disable** or **Enable** for **Inline Power**.
4. Click **Class** for **Allocate Power By** and then select a power class in the **Class** list, or click **Power Limit** and then type the maximum power level for a power-consuming device in the **Power Limit** field.
5. Select an inline power priority for a Power over Ethernet (PoE) port in the **Priority** list.
6. To select the PoE ports, select the **Select a range** check box and select the range of ports in the **From** and **To** lists, or select the **Select one port** check box and select the port in the list.

7. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

To display the inline power statistics and details, click **Show Inline Power**. For more information, refer to "Displaying port inline power for Brocade FCX and Brocade ICX 6610 devices" on page 44.

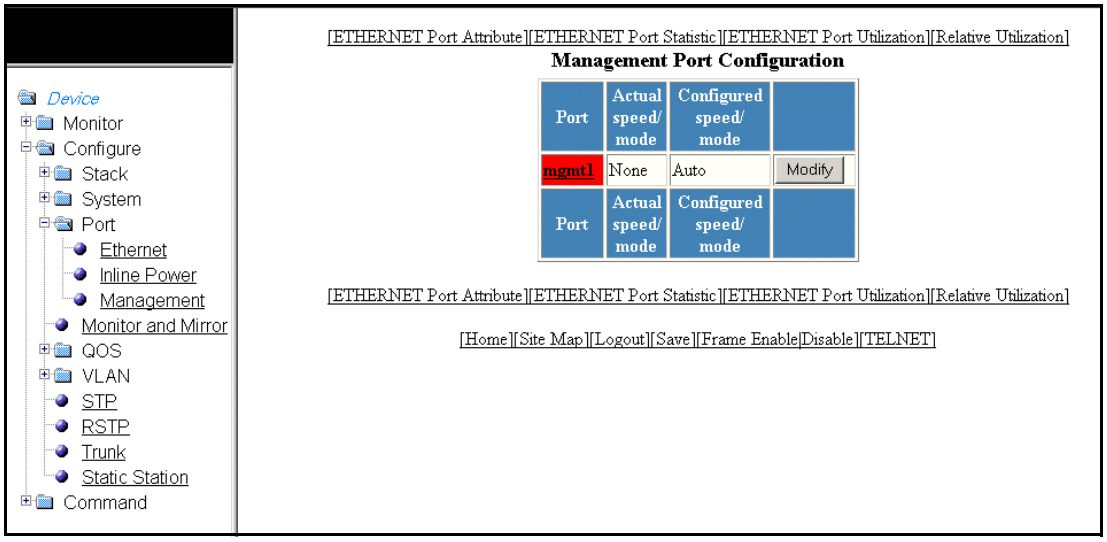
Configuring a management port

To configure a management port, perform the following steps.

1. Click **Configure** on the left pane and select **Port**.
2. Click **Management**.

The **Management Port Configuration** window is displayed as shown in Figure 114.

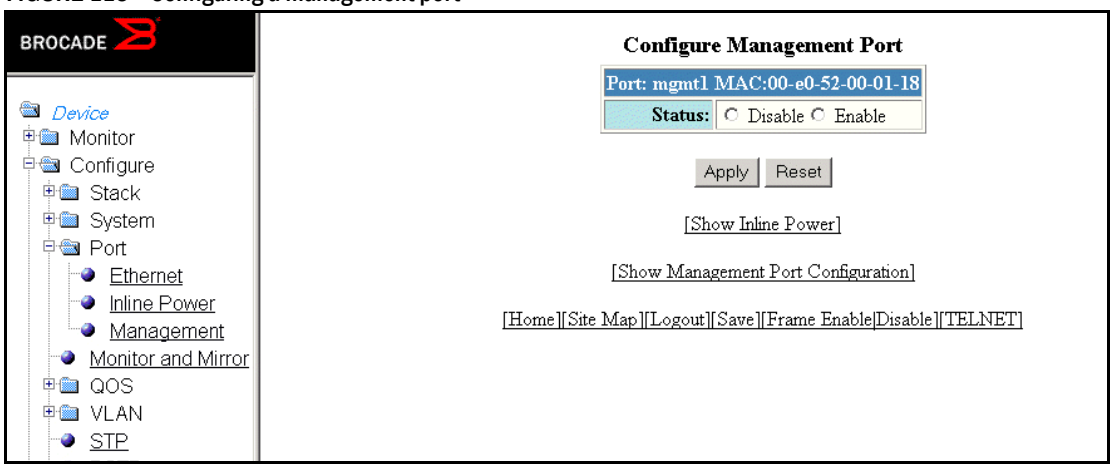
FIGURE 114 Management port configuration



3. Click **Modify**.

The **Configure Management Port** window is displayed as shown in Figure 115.

FIGURE 115 Configuring a management port



4. Click **Disable** or **Enable** for **Status**.
5. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

To display the configured management port information, click **Show Management Port Configuration**.

To display the inline power statistics and details, click **Show Inline Power**. For more information, refer to "Displaying port inline power for Brocade FCX and Brocade ICX 6610 devices" on page 44.

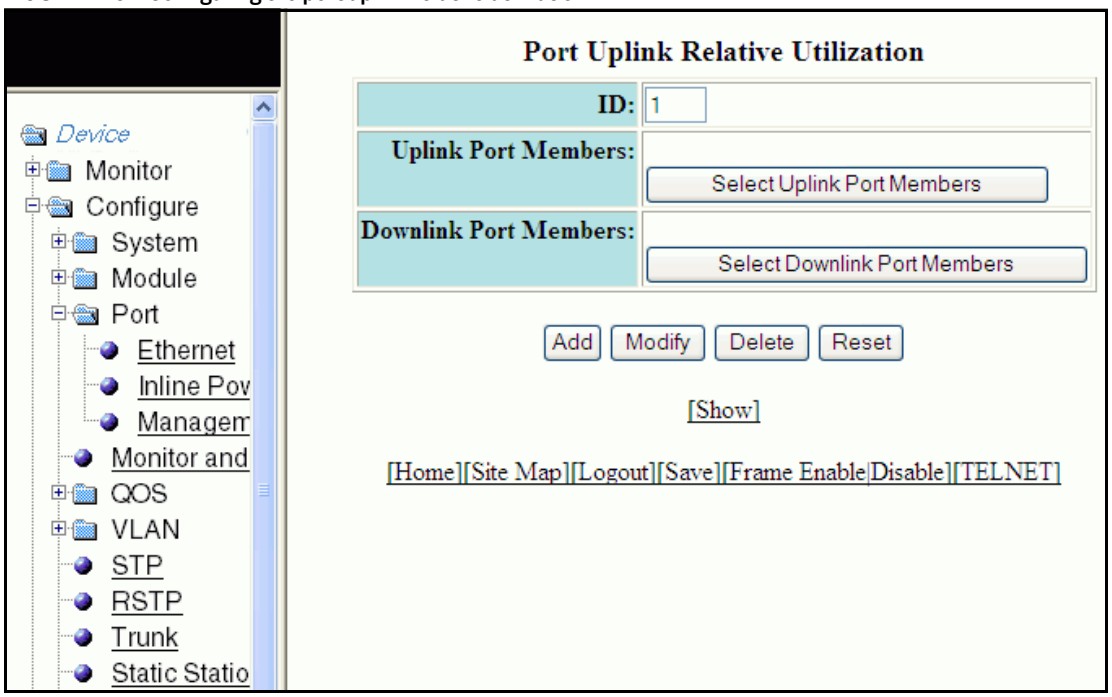
Configuring the port uplink relative utilization

To configure the port uplink utilization list, perform the following steps.

1. Click **Configure** on the left pane and select **Port**.
2. Click **Relative Utilization** on the **ETHERNET Port Configuration**, **Configure Inline Power**, or **Management Port Configuration** window.

The **Port Uplink Relative Utilization** window is displayed as shown in Figure 116.

FIGURE 116 Configuring the port uplink relative utilization



3. Type the uplink utilization list number (from 1 through 4) in the **ID** field.
4. Click **Select Uplink Port Members** to select the uplink ports.
5. Click **Select Downlink Port Members** to select the downlink ports.

NOTE
The port number varies based on the product:

- For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
- For Brocade FSX devices – slotnum/portnum

6. Click **Add**.

The message **The change has been made** is displayed. To display the configured port uplink utilization list, click **Show**.

To modify the configured port uplink utilization list, click **Modify**. You can also delete configured port uplink utilization list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

18

Configuring Monitor and Mirror Port

In this chapter

- Configuring a mirror port 181
- Configuring a monitor port 182

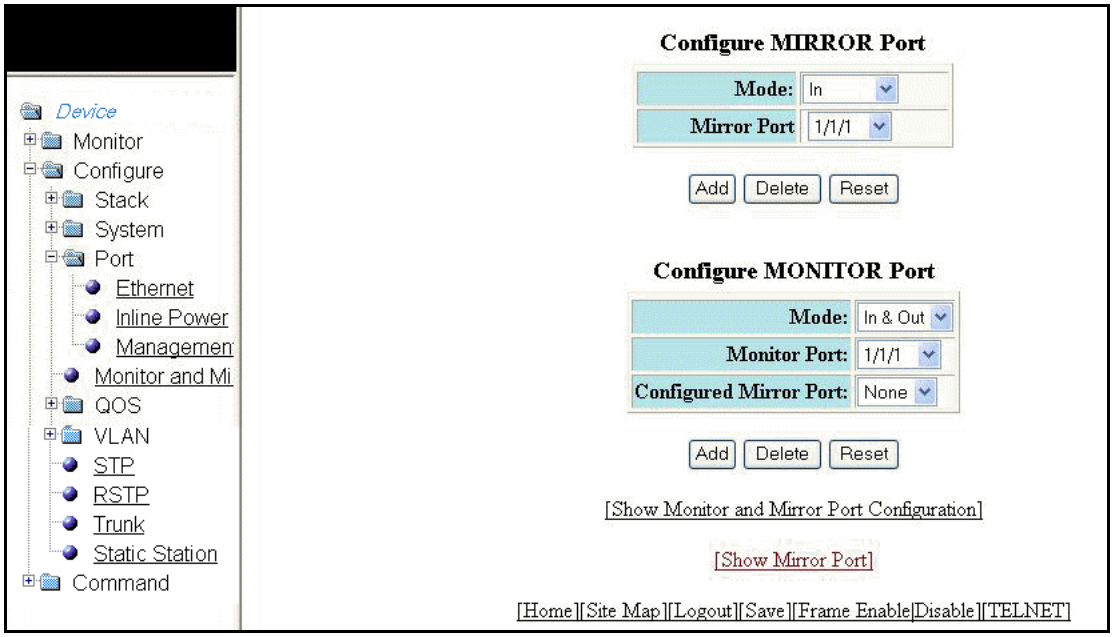
Configuring a mirror port

To configure port monitoring, first configure the mirror port. The mirror port is the port to which the monitored traffic is copied. To configure a mirror port, perform the following steps.

1. Click **Configure** on the left pane and select **Monitor and Mirror**.

The **Configure MIRROR Port** window is displayed as shown in Figure 117.

FIGURE 117 Configuring a mirror port



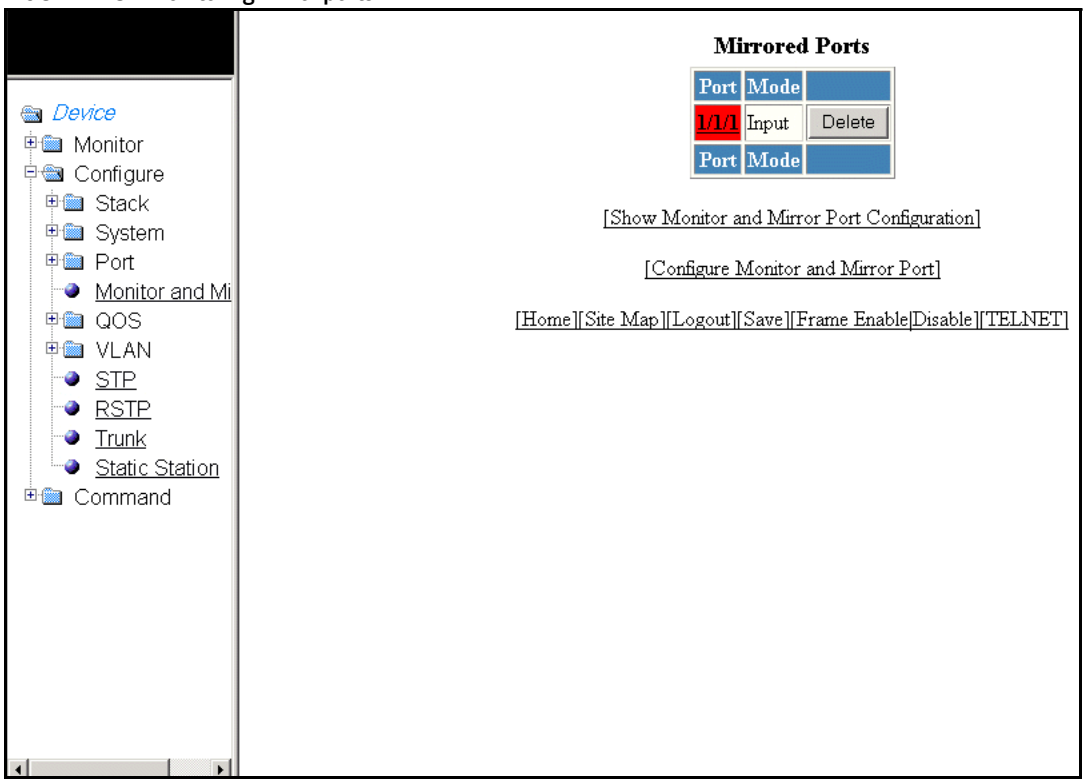
2. Select the mode in which the port operates in the **Mode** list, which can be one of the following:
   - **In**
   - **Out**
   - **In & Out**

3. Select a port to which the monitored traffic must be copied in the **Mirror Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Click **Add**.

The message **The change has been made** is displayed. To display the configured mirror port, click **Show Mirror Port**. Figure 118 shows the **Mirrored Ports** window with the configured mirror port information.

To delete the configured mirror port, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

FIGURE 118 Monitoring mirror ports



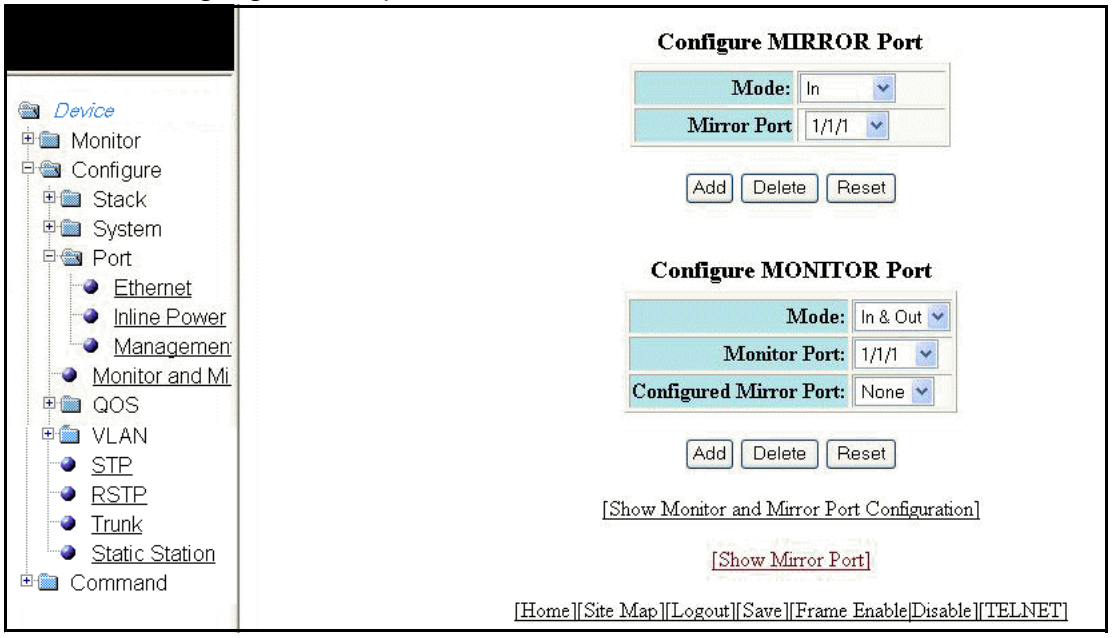
Configuring a monitor port

To configure port monitoring on an individual port on a Brocade device, perform the following steps.

1. Click **Configure** on the left pane and select **Monitor and Mirror**.

The **Configure MONITOR Port** window is displayed as shown in Figure 119.

FIGURE 119 Configuring the monitor port



2. Select one of the following modes in which the port operates in the **Mode** list:
   - **In**
   - **Out**
   - **In & Out**
3. Select a port for which you want to monitor the traffic in the **Monitor Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Select a mirror port that you have configured in the **Configured Mirror Port** list.
5. Click **Add**.

The message **The change has been made** is displayed. To display the configured monitor port, click **Show Monitor and Mirror Port Configuration**. To display the mirror port, click **Show Mirror Port**.

To delete the configured monitor port, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

Configuring QoS

19

In this chapter

- Configuring the QoS profile 185
- Configuring the QoS profile bind. 186

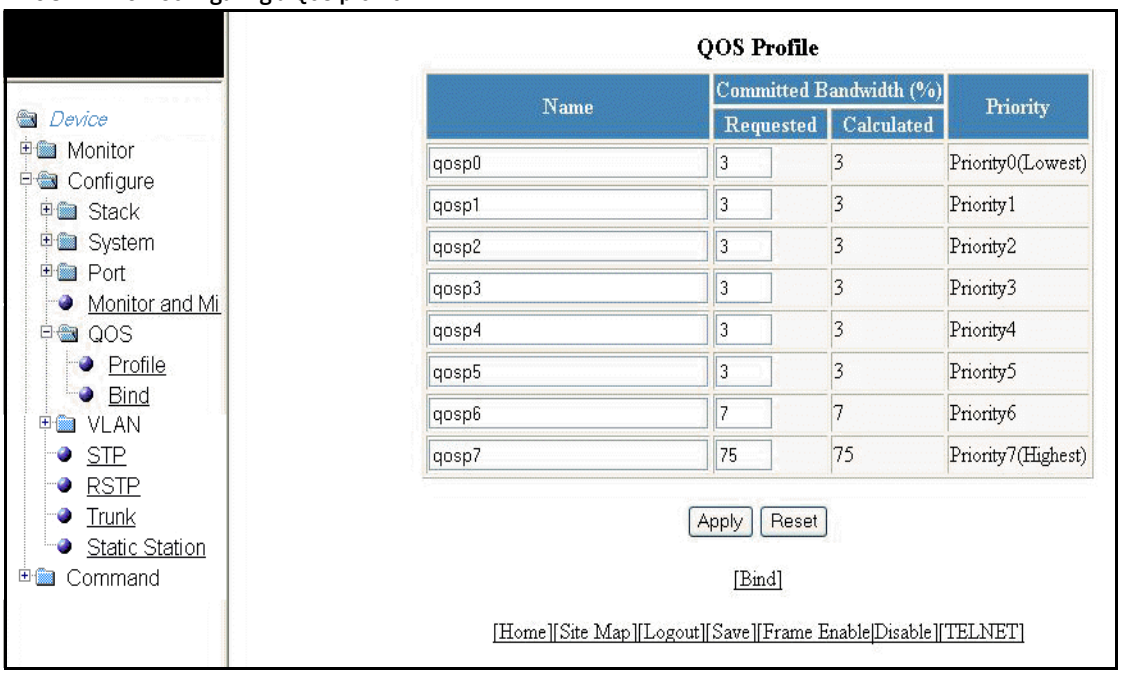
Configuring the QoS profile

To configure the Quality of Service (QoS) profile, perform the following steps.

1. Click **Configure** on the left pane and select **QOS**.
2. Click **Profile**.

The **QOS Profile** window is displayed as shown in Figure 120.

FIGURE 120 Configuring a QoS profile



3. The default queue names are **qosp0**, **qosp1**, **qosp2**, **qosp3**, **qosp4**, **qosp5**, **qosp6**, and **qosp7**. You can change one or more of the names, if desired. Type the QoS name in the **Name** field.
4. The **Committed Bandwidth (%)** is the percentage of the device outbound bandwidth that is allocated to the queue. Brocade QoS queues require a minimum bandwidth of 3 percent for each priority. Type the percentage of bandwidth you want for the queue in the **Requested** field.

NOTE
The total of the percentages you enter must be equal to 100. The Brocade device does not adjust the bandwidth percentages you enter.

5. Click **Apply**.

The message **The change has been made** is displayed and the committed bandwidth is changed to the configured value in the **Calculated** field. The **Priority** field shows the default priority of the individual QoS from lowest to highest (0 through 7).

To clear the entered data in the fields, click **Reset**. To configure the QoS profile bind, click **Bind**. For more information on how to configure a QoS profile bind, refer to "Configuring the QoS profile bind" on page 186.

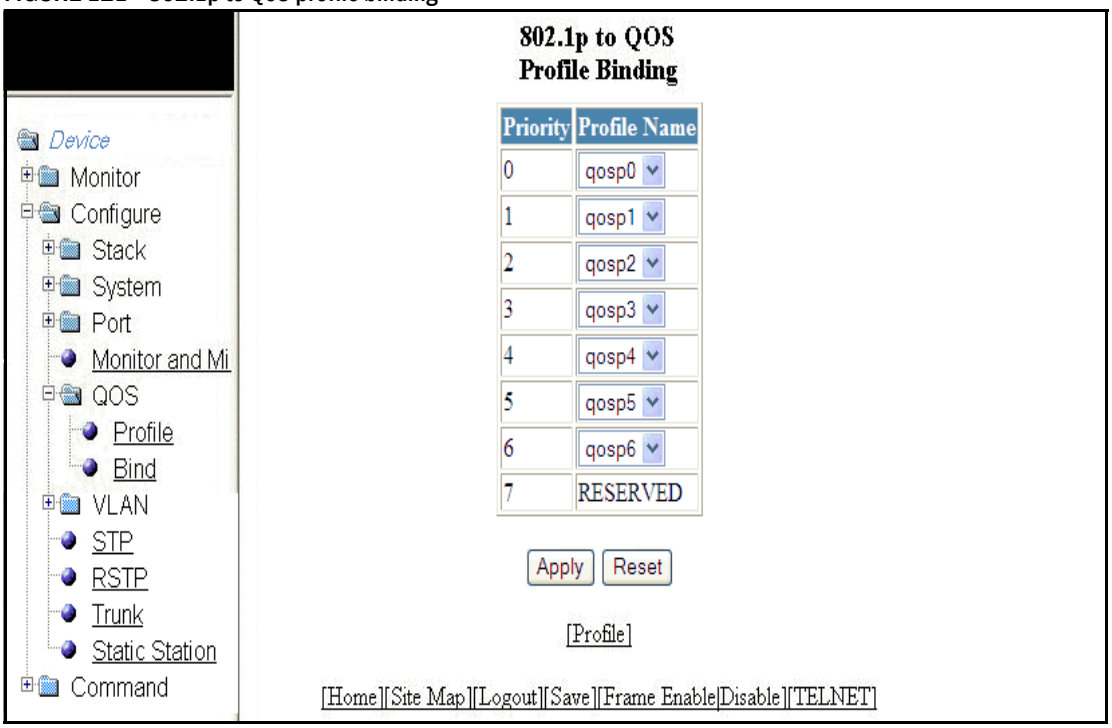
Configuring the QoS profile bind

To bind an 802.1p priority to a hardware forwarding queue, perform the following steps.

1. Click **Configure** on the left pane and select **QOS**.
2. Click **Bind**.

The **802.1p to QOS Profile Binding** window is displayed as shown in Figure 121.

FIGURE 121 802.1p to QoS profile binding



3. Select a hardware forwarding queue to which you are reassigning the priority in the **Profile Name** lists.
4. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

To configure the Quality of Service (QoS) profile, click **Profile**. For more information, refer to "Configuring the QoS profile" on page 185.

Chapter

Configuring VLAN

20

In this chapter

- Configuring a port VLAN for Brocade FCX and Brocade ICX 6610 devices 189
- Modifying a port VLAN 192
- Configuring a port VLAN for Brocade FSX devices 194
- Configuring a protocol VLAN 196

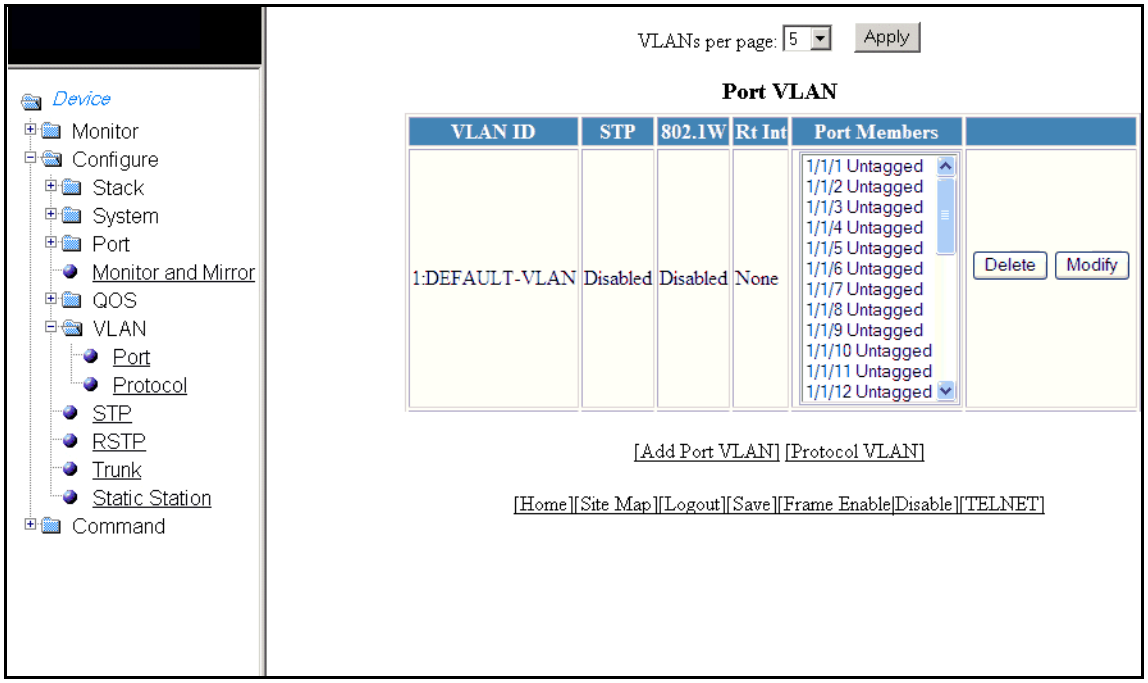
Configuring a port VLAN for Brocade FCX and Brocade ICX 6610 devices

To configure a port-based Virtual LAN (VLAN) for Brocade FCX and Brocade ICX 6610 devices, perform the following steps.

1. Click **Configure** on the left pane and select **VLAN**.
2. Click **Port**.

The **Port VLAN** window is displayed as shown in Figure 122. You can limit the number of VLANs displayed per page using the **VLANs per page** list.

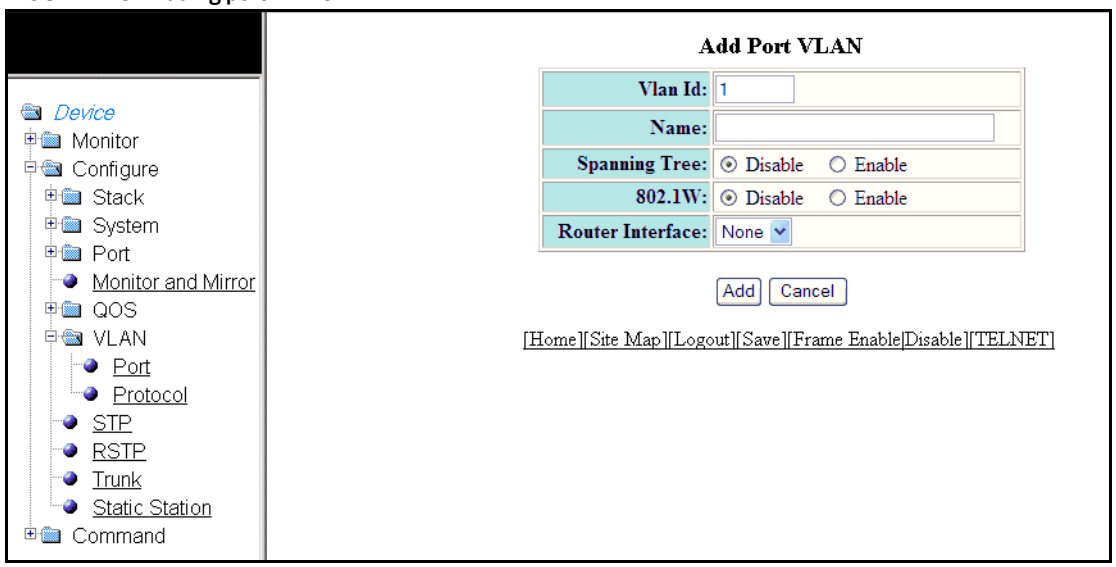
FIGURE 122 Configuring port VLANs



3. Click **Add Port VLAN**.

The **Add Port VLAN** window is displayed as shown in Figure 123.

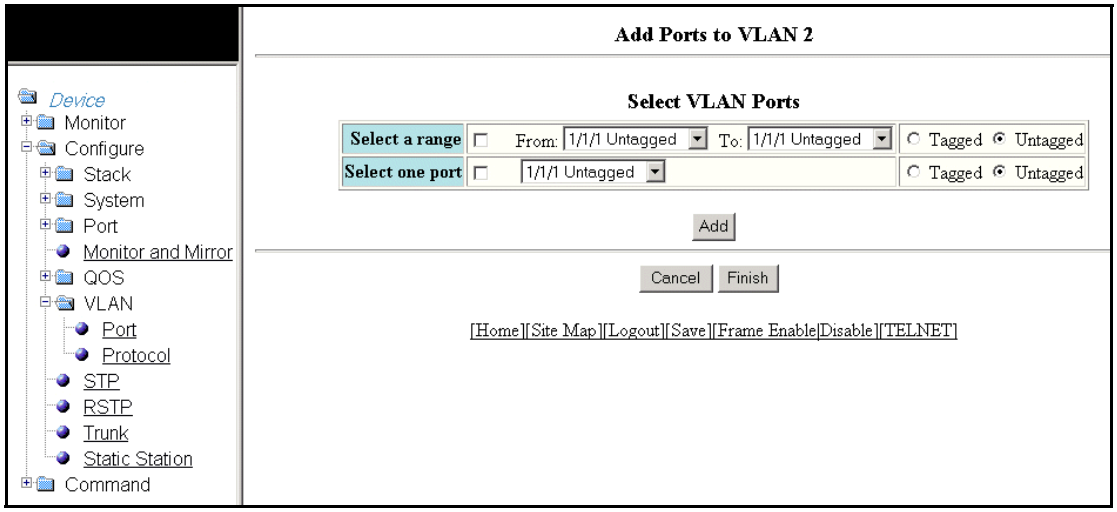
FIGURE 123 Adding port VLANs



4. Type the VLAN identifier of the port in the **Vlan Id** field.
5. Type the port VLAN name in the **Name** field.
6. Click **Disable** or **Enable** for **Spanning Tree**.
7. Click **Disable** or **Enable** for **802.1W**.
8. Select a virtual routing interface in the **Router Interface** list.
9. Click **Add**.

The **Add Ports to VLAN** window is displayed as shown in Figure 124.

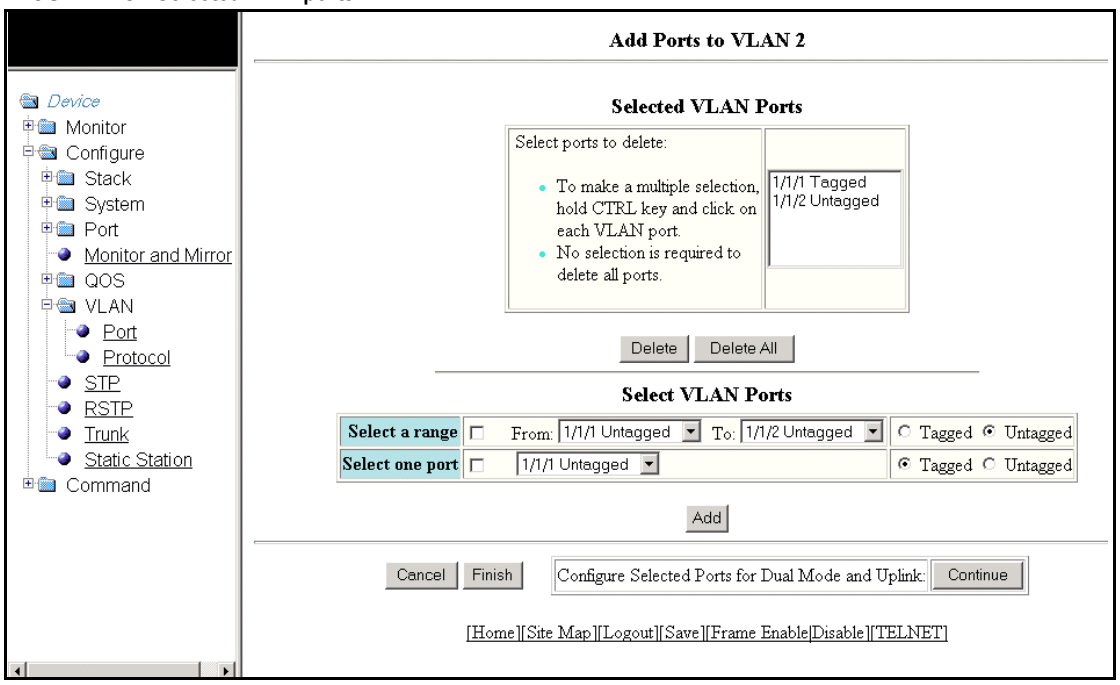
FIGURE 124 Adding ports to VLANs



10. To select the VLAN ports, select the **Select a range** check box, select the range of VLAN ports in the **From** and **To** lists, and click **Tagged** or **Untagged**, or select the **Select one port** check box, select a port-based VLAN in the list, and click **Tagged** or **Untagged**.
11. Click **Add**.

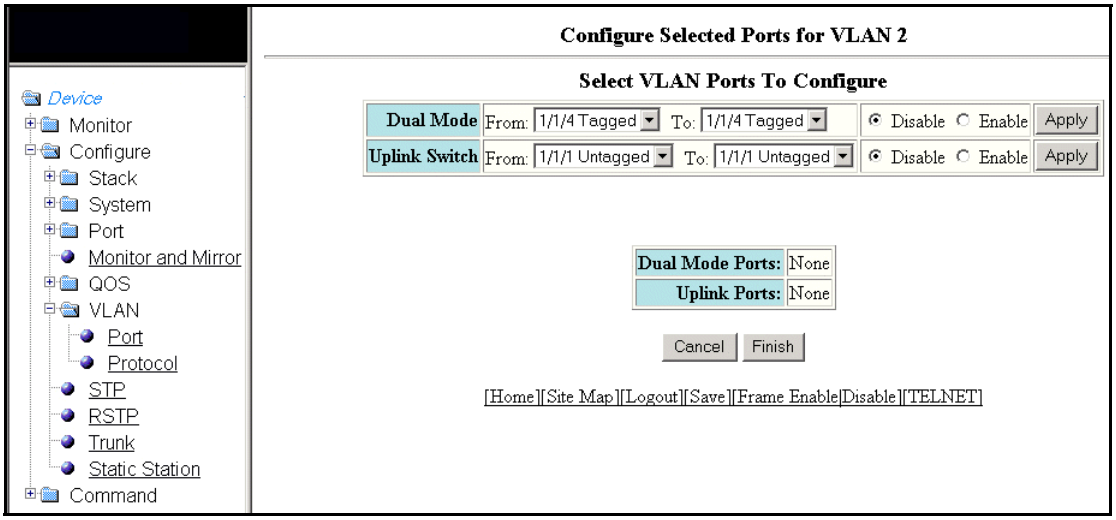
The **Selected VLAN Ports** window is displayed as shown in Figure 125.

FIGURE 125 Selected VLAN ports



12. The selected VLAN ports are displayed in the **Selected VLAN Ports** list. Click **Delete** or **Delete All** to delete the VLAN ports.
13. You can add more VLAN ports from the **Select VLAN Ports** pane. To do so, complete step 10 and step 11.
14. Click **Finish** to return to the **Port VLAN** window with the configured port-based VLAN displayed, or click **Continue** to configure selected ports for dual mode and uplink. The **Configure Selected Ports for VLAN** window is displayed as shown in Figure 126.

FIGURE 126 Configuring dual mode and uplink for ports



15. To configure dual mode and uplink for the ports, perform the following steps.

    a. Select the ports for which you want to configure the dual mode in the **From** and **To** lists for **Dual Mode**. Click **Disable** or **Enable** and then click **Apply**. The configured ports are displayed in the **Dual Mode Ports** list.

    b. Select the ports for which you want to configure uplink in the **From** and **To** lists for **Uplink Switch**. Click **Disable** or **Enable** and then click **Apply**. The configured ports are displayed in the **Uplink Ports** list.

    c. Click **Finish**.

The configured port VLAN is displayed in the **Port VLAN** window. To cancel the VLAN port configuration and return to the **Port VLAN** window, click **Cancel**.

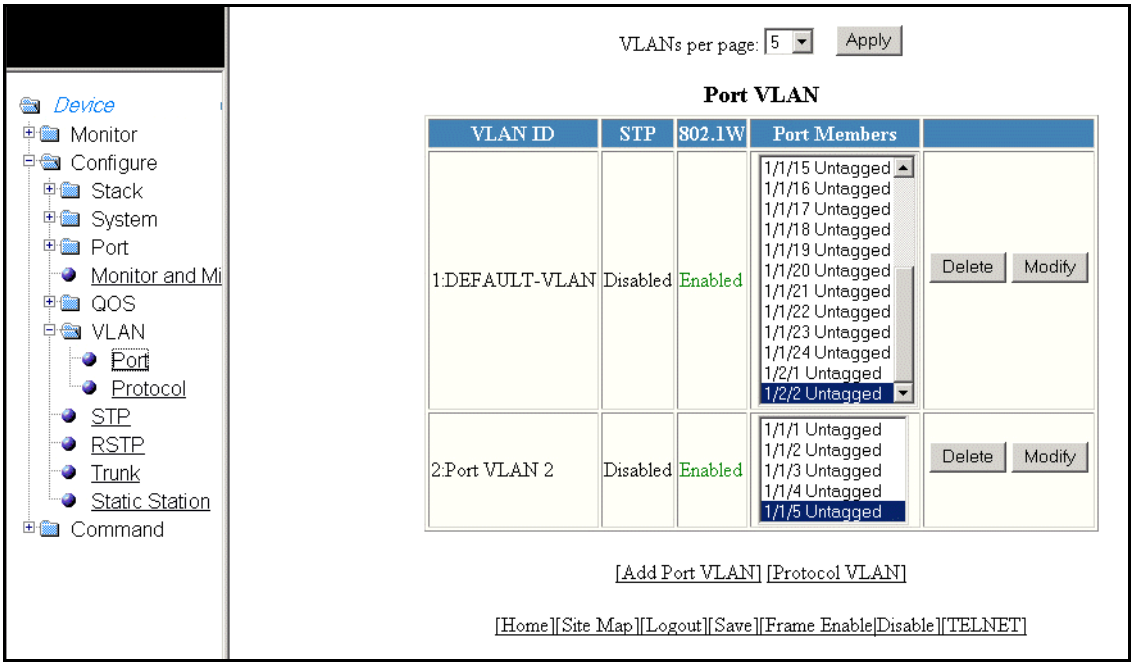
Modifying a port VLAN

To modify a port VLAN, perform the following steps.

1. Click **Configure** on the left pane and select **VLAN**.
2. Click **Port**.

The **Port VLAN** window is displayed as shown in Figure 127.

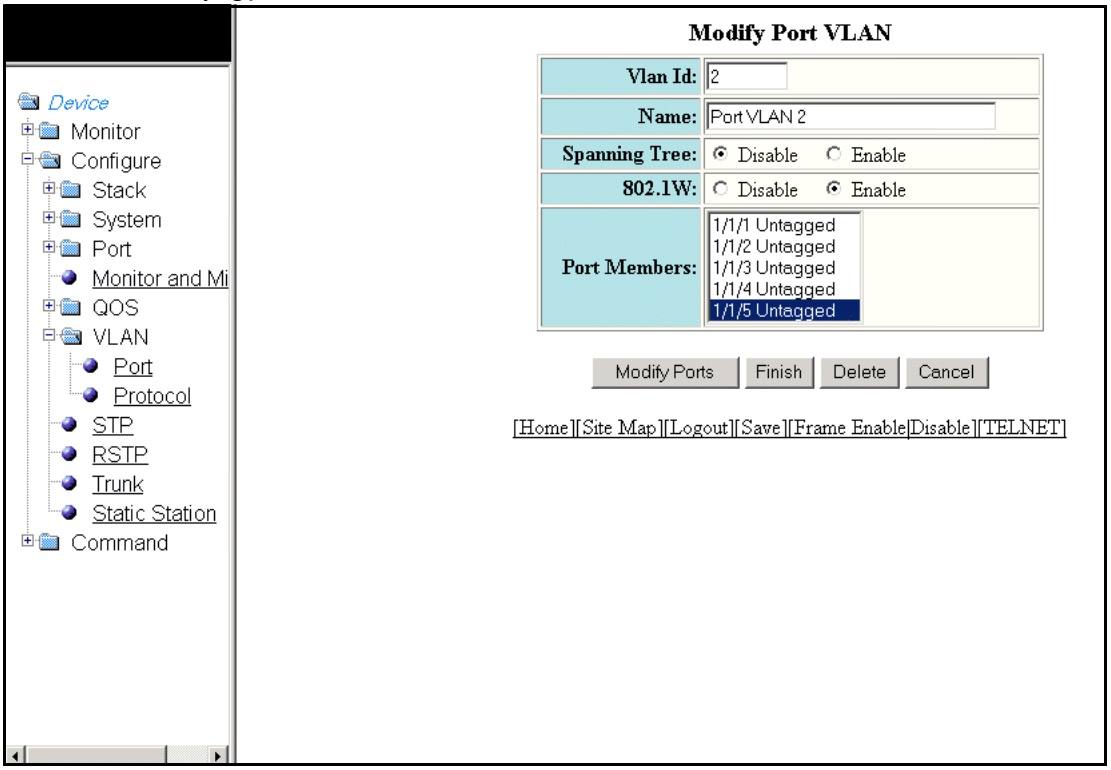
FIGURE 127 Configuring port VLANs



3. Click **Modify**.

The **Modify Port VLAN** window is displayed as shown in Figure 128.

FIGURE 128 Modifying port VLANs



4. Type the VLAN identifier of the port in the **Vlan Id** field.

5. Type the port VLAN name in the **Name** field.
6. Click **Disable** or **Enable** for **802.1W**.
7. Select the VLAN ports in the **Port Members** list.
8. Click **Modify Ports** to add or delete VLAN ports.
9. Click **Finish**.

To delete the configured port VLAN, click **Delete**. To undo your changes and go back to the **Port VLAN** window, click **Cancel**.

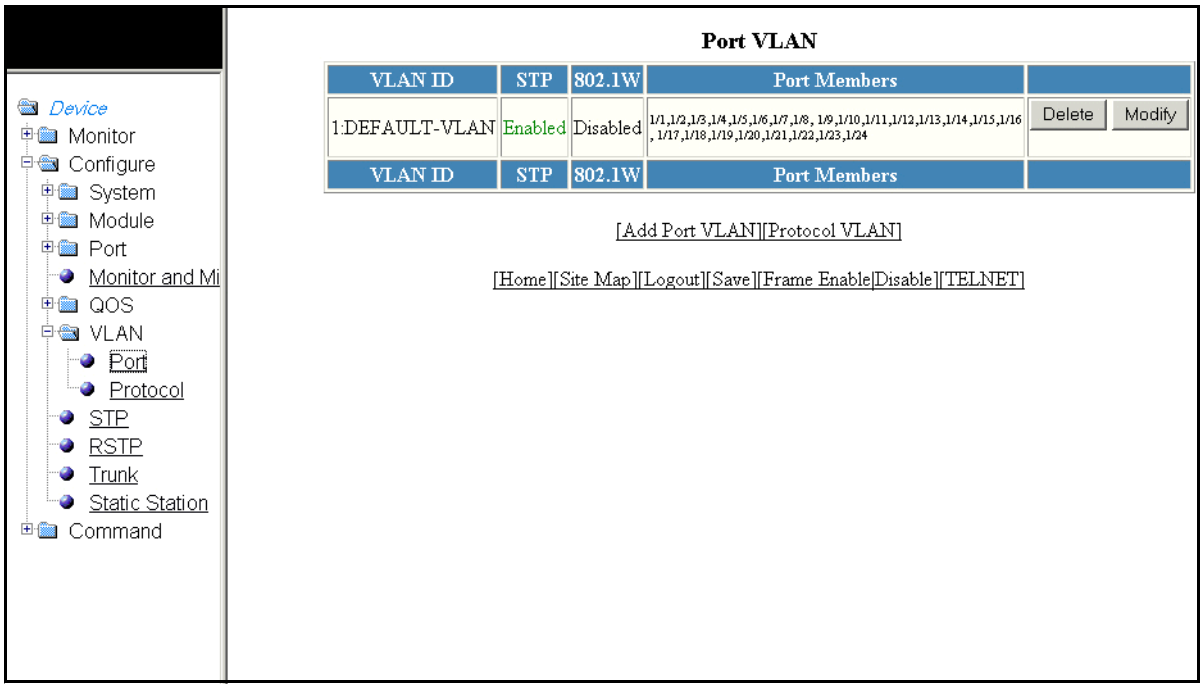
Configuring a port VLAN for Brocade FSX devices

To configure a port-based Virtual LAN (VLAN) for Brocade FSX devices, perform the following steps.

1. Click **Configure** on the left pane and select **VLAN**.
2. Click **Port**.

The **Port VLAN** window is displayed as shown in Figure 129.

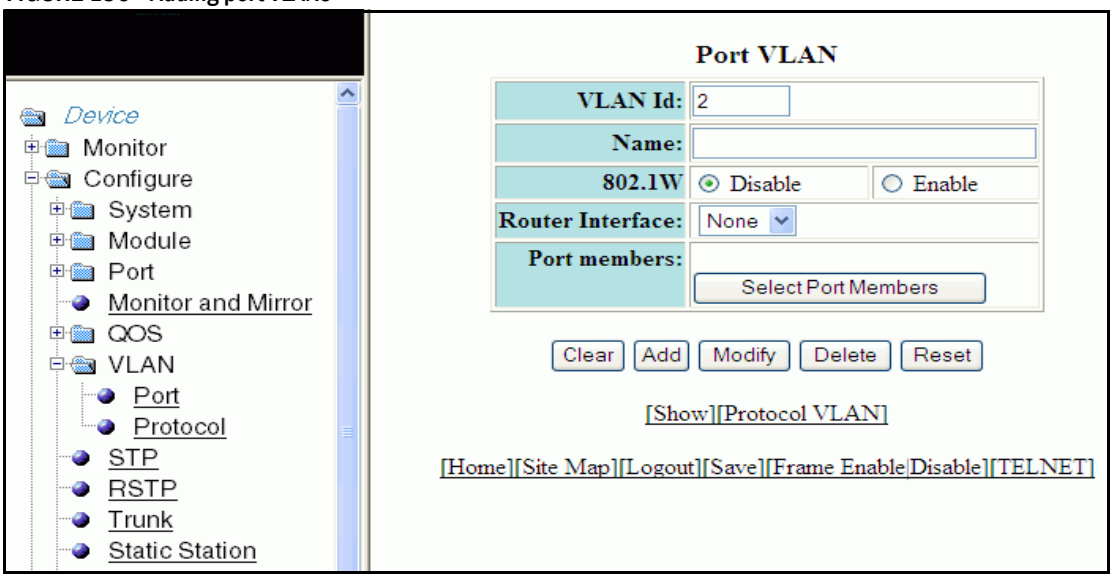
FIGURE 129 Configuring port VLANs



3. Click **Add Port VLAN**.

The **Add Port VLAN** window is displayed as shown in Figure 130.

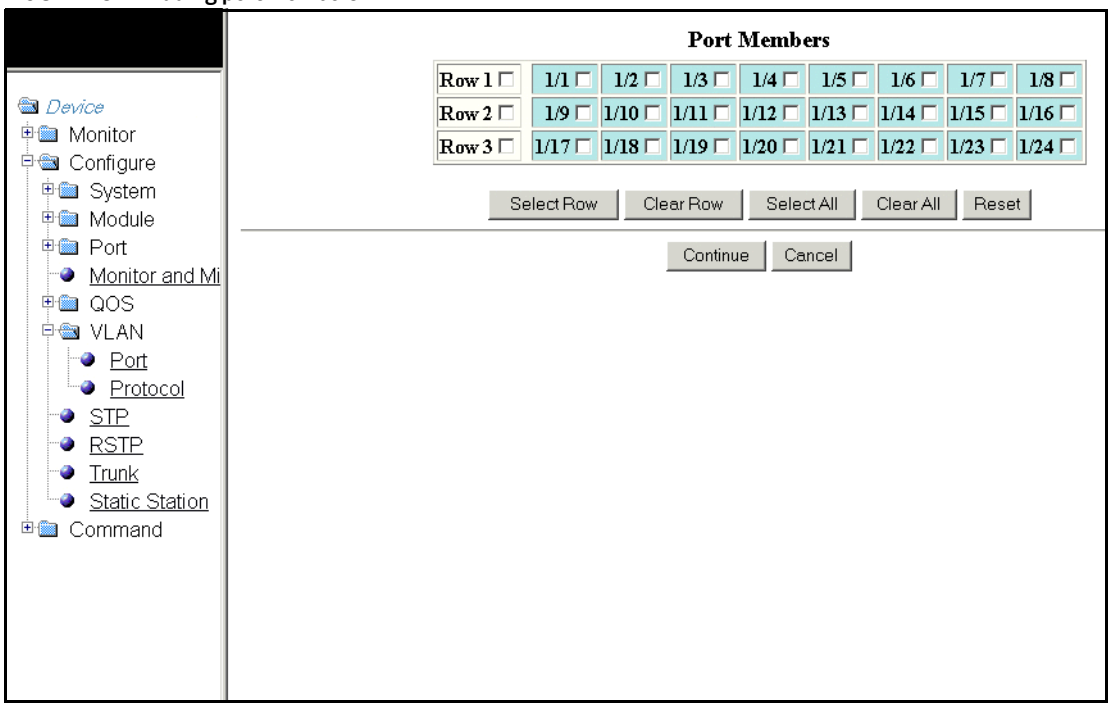
FIGURE 130 Adding port VLANs



4. Type the VLAN identifier of the port in the **VLAN Id** field.
5. Type the port VLAN name in the **Name** field.
6. Click **Disable** or **Enable** for **802.1W**.
7. Select a virtual routing interface in the **Router Interface** list.
8. Click **Select Port Members** to add ports to the VLAN.

The **Port Members** window is displayed as shown in Figure 131.

FIGURE 131 Adding port members



The options within the right panel include the following:

- **Select Row** - Allows you to select the entire row.
- **Clear Row** - Allows you to clear any selected row.
- **Select All** - Allows you to select all the port members.
- **Clear All** - Allows you to clear all the port members selected.
- **Reset** - Allows you to undo your changes.

9. Select the port members and click **Continue**. The **Port VLAN** window is displayed and the selected port members are displayed in the **Port Members** field. To cancel the selection of the ports and go back to the **Port VLAN** window, click **Cancel**.
10. Click **Add**.

The message **The change has been made** is displayed. To delete the configured port VLAN, click **Delete**. To undo your changes and go back to the **Port VLAN** window, click **Cancel**.

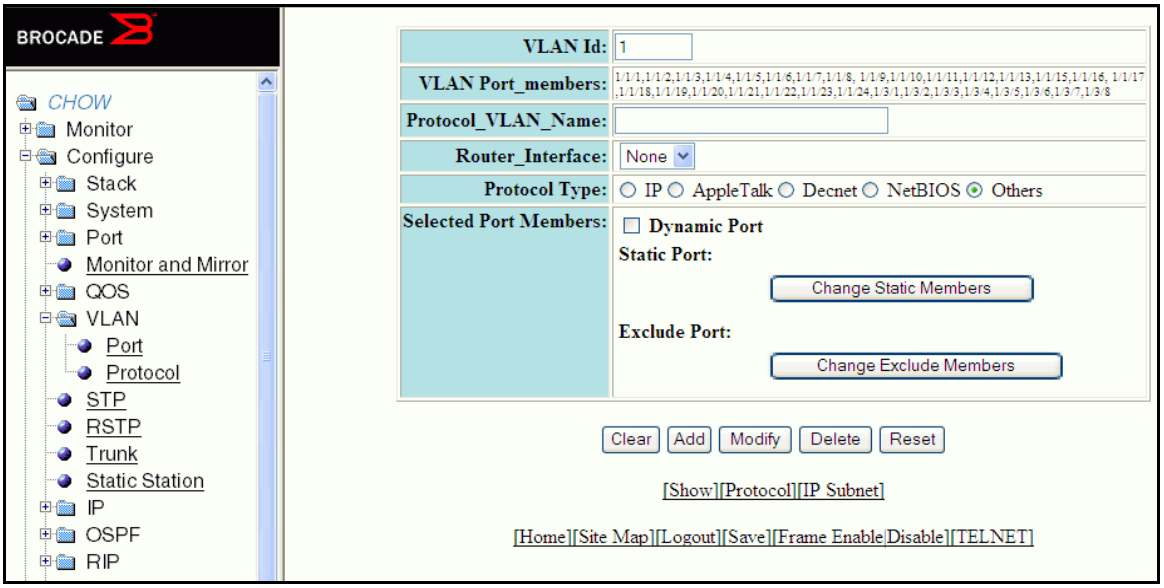
Configuring a protocol VLAN

To configure a protocol-based VLAN, perform the following steps.

1. Click **Configure** on the left pane and select **VLAN**.
2. Click **Protocol**.

The protocol VLAN window is displayed as shown in Figure 132.

FIGURE 132 Configuring a protocol VLAN

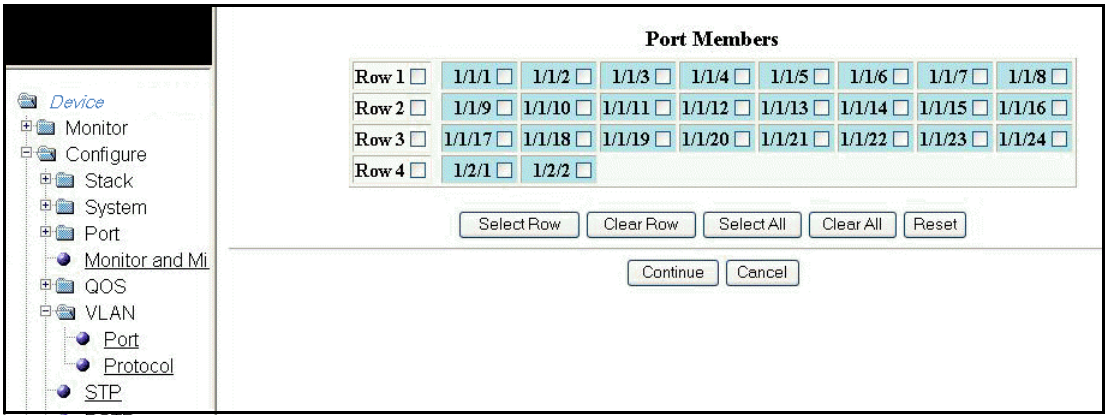


3. Type the VLAN identifier in the **VLAN Id** field.
4. Type the VLAN name in the **Protocol_VLAN_Name** field.
5. Select a virtual routing interface in the **Router Interface** list.

6. Click one of the following types for **Protocol Type**:
   - **IP** – The device sends IP broadcasts to all ports within the IP protocol VLAN.
   - **IPX** – The device sends IPX broadcasts to all ports within the IPX protocol VLAN.
   - **AppleTalk** – The device sends AppleTalk broadcasts to all ports within the AppleTalk protocol VLAN.
   - **Decnet** – The device sends DECnet broadcasts to all ports within the DECnet protocol VLAN.
   - **NetBIOS** – The device sends NetBIOS broadcasts to all ports within the NetBIOS protocol VLAN.
   - **Other** – The device sends broadcasts from all protocol types other than those listed in **Protocol Type** to all ports within the VLAN.
7. Select the **Dynamic Port** check box to add the protocol VLAN dynamically.
8. Click **Change Static Members** to add protocol VLANs statically.

The **Port Members** window is displayed as shown in Figure 133.

FIGURE 133 Adding static port members



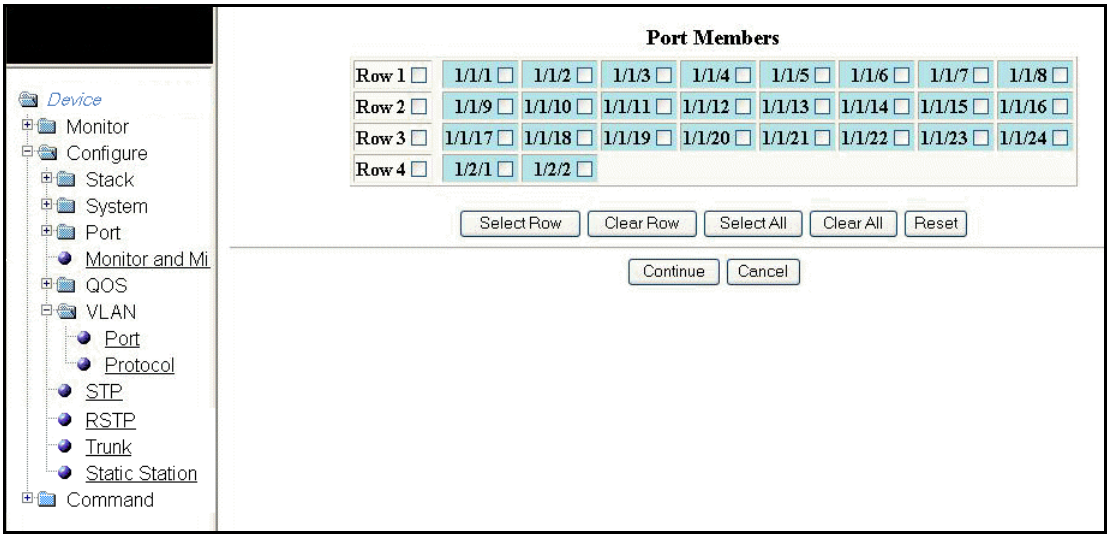
The options within the right panel include the following:

- **Select Row** - Allows you to select the entire row.
- **Clear Row** - Allows you to clear any selected row.
- **Select All** - Allows you to select all the port members.
- **Clear All** - Allows you to clear all the port members selected.
- **Reset** - Allows you to undo your changes.

9. Select the port members and click **Continue** to view the selected port members as shown in Figure 134. To go back to the protocol VLAN window, click **Cancel**.
10. Click **Change Exclude Members** to explicitly exclude the selected ports in a port-based VLAN from becoming members of a protocol.

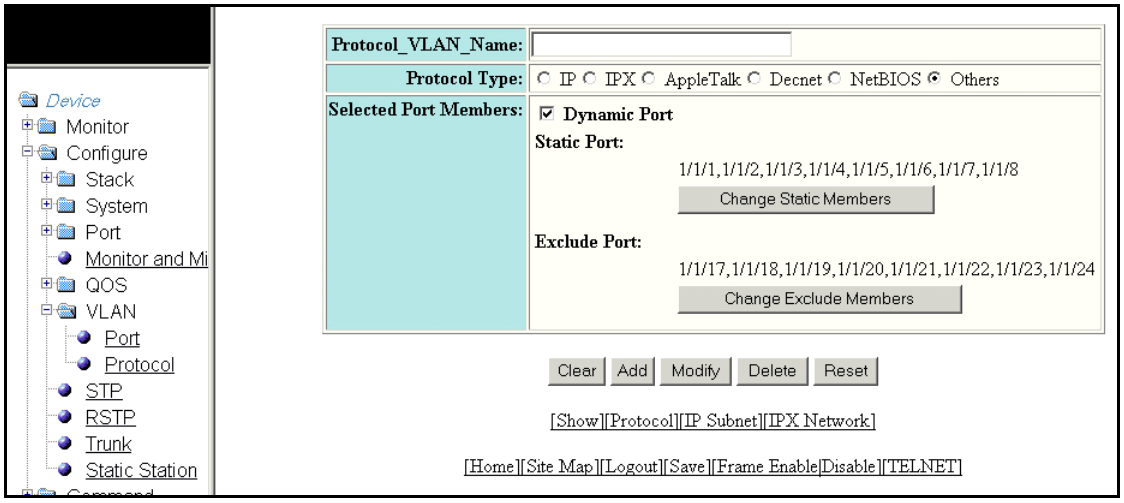
The Port Members window is displayed as show in Figure 134.

FIGURE 134 Excluding port members



11. Select the port members and click **Continue** to view the selected port members as shown in Figure 135.

FIGURE 135 Displaying the selected port members



12. Click **Add**.

The message **The change has been made** is displayed. To display the configured protocol VLAN, click **Show**.

To modify the configured protocol VLAN, click **Modify**. You can also delete the protocol VLAN by clicking **Delete**. To clear the selected static and exclude ports, click **Clear**. To reset the data entered in the configuration pane, click **Reset**.

Configuring an IP subnet VLAN

To configure an IP subnet VLAN, perform the following steps.

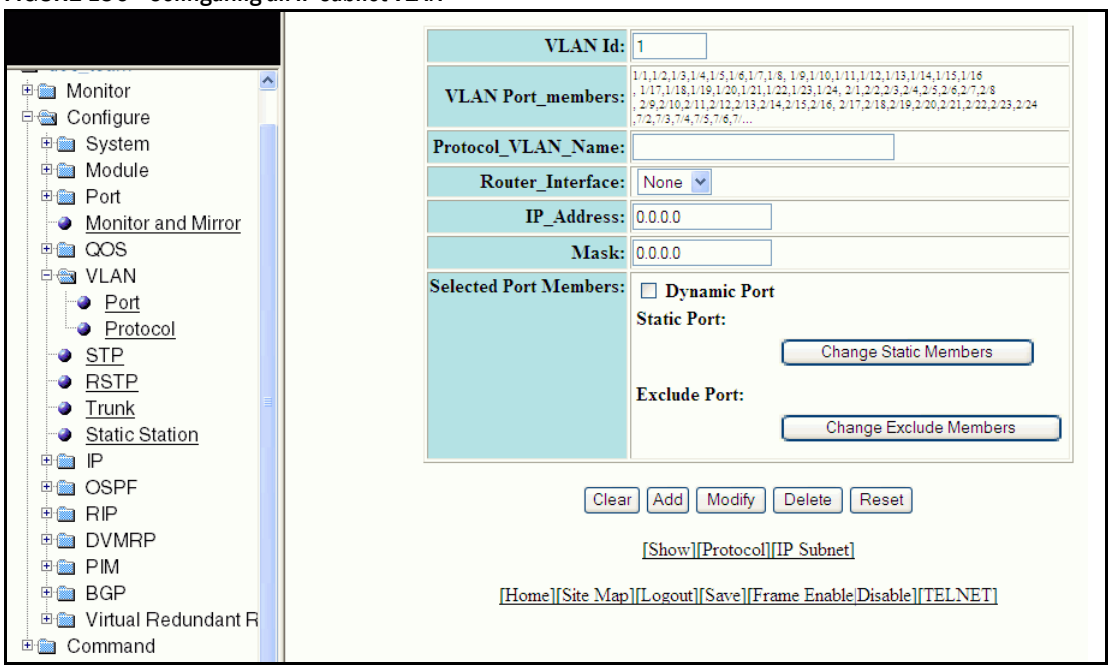
1. Click **Configure** on the left pane and select **VLAN**.
2. Click **Protocol**.

The protocol VLAN window is displayed as shown in Figure 132.

3. Click **IP Subnet**.

The IP subnet VLAN window is displayed as shown in Figure 136.

FIGURE 136 Configuring an IP subnet VLAN



4. Type the VLAN identifier in the **VLAN Id** field.
5. Type the protocol-based VLAN name in the **Protocol_VLAN_Name** field.
6. Select a virtual routing interface in the **Router Interface** list.
7. Type the IP address of the device in the **IP_Address** field.
8. Type the IP subnet mask in the **Mask** field. This parameter provides a filter for displaying multiple MAC addresses that have specific values in common.
9. Select the **Dynamic Port** check box to add the IP subnet VLANs dynamically.
10. Click **Change Static Members** to add IP subnet VLANs statically.
11. Click **Change Exclude Members** to explicitly exclude the selected ports in a port-based VLAN from becoming members of an IP subnet.
12. Click **Add**.

The message **The change has been made** is displayed. To display the configured IP subnet VLAN, click **Show**.

To modify the configured IP subnet VLAN, click **Modify**. You can also delete the IP subnet VLAN by clicking **Delete**. To clear the selected static and exclude ports, click **Clear**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

21

Configuring STP

In this chapter

- Configuring STP parameters 201

Configuring STP parameters

Brocade Layer 2 switches and Layer 3 switches support standard Spanning Tree Protocol (STP) as described in the IEEE 802.1D specification.

Each port-based VLAN on a Brocade device runs a separate spanning tree. A Brocade device has one port-based VLAN (VLAN 1) that contains all the device ports. However, if you configure additional port-based VLANs on a Brocade device, then each of those VLANs on which STP is enabled and the VLAN 1 run separate spanning trees.

If you configure a port-based VLAN on the device, the VLAN has the same STP state as the default STP state on the device. Thus, by default on Layer 2 switches, new VLANs have STP enabled and on Layer 3 switches, new VLANs have STP disabled. You can enable or disable STP in each VLAN separately and also on individual ports.

Using the Web Management Interface, you can change the default STP bridge and port parameters.

Changing STP bridge parameters

Table 52 lists the default STP bridge parameters.

TABLE 52 Default STP bridge parameters

Parameter	Default value
Forward Delay	15 seconds
Maximum Age	20 seconds
Hello Time	2 seconds
Priority	32768

NOTE
To change STP bridge timers, you must stay within the following ranges:

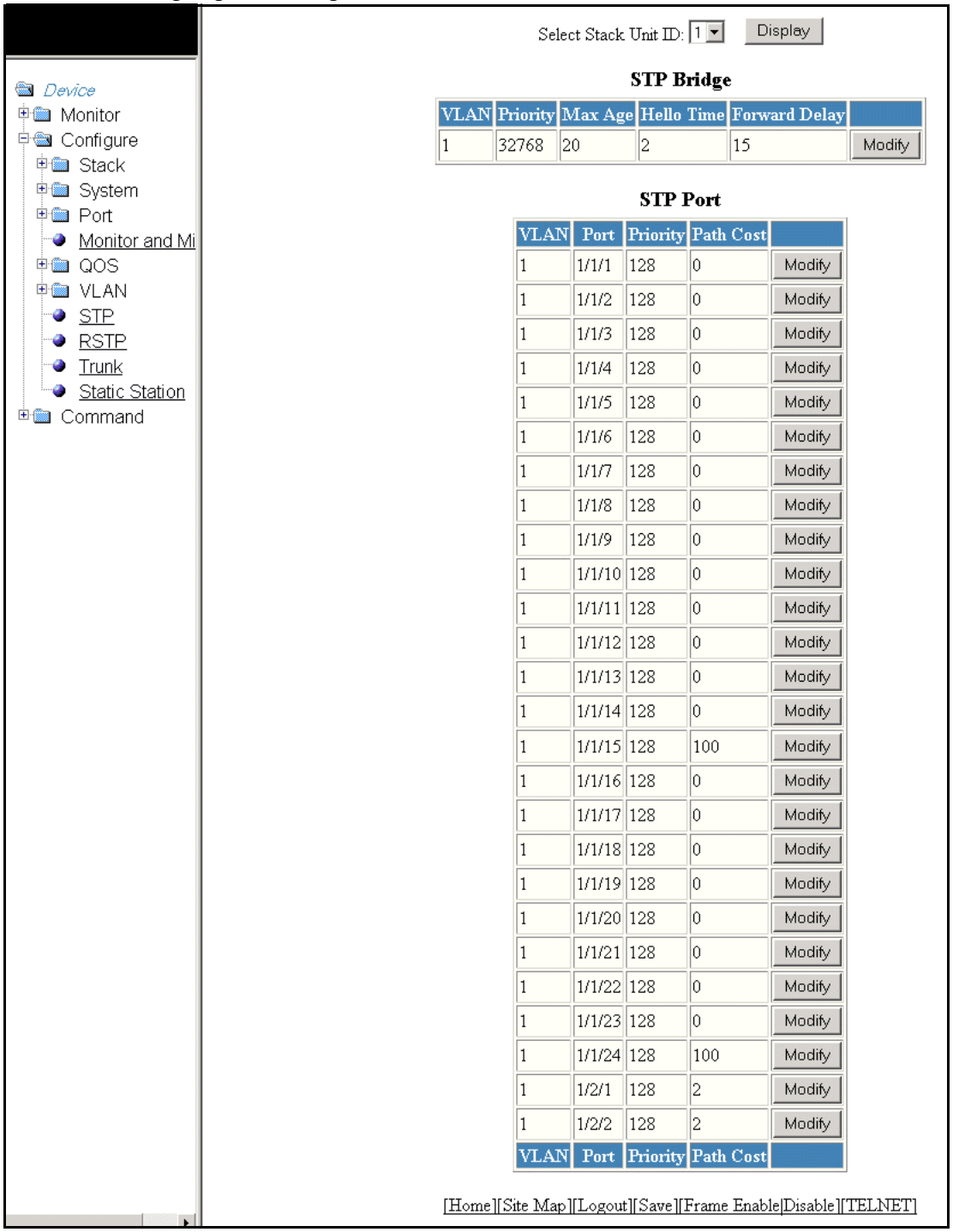
2 * (Forward Delay-1) >= Maximum Age >= 2 * (Hello Time +1)

To change the default STP bridge values, perform the following steps.

1. Click **Configure** on the left pane and select **STP**.

The **STP Bridge** window is displayed as shown in Figure 137.

FIGURE 137 Configuring the STP bridge



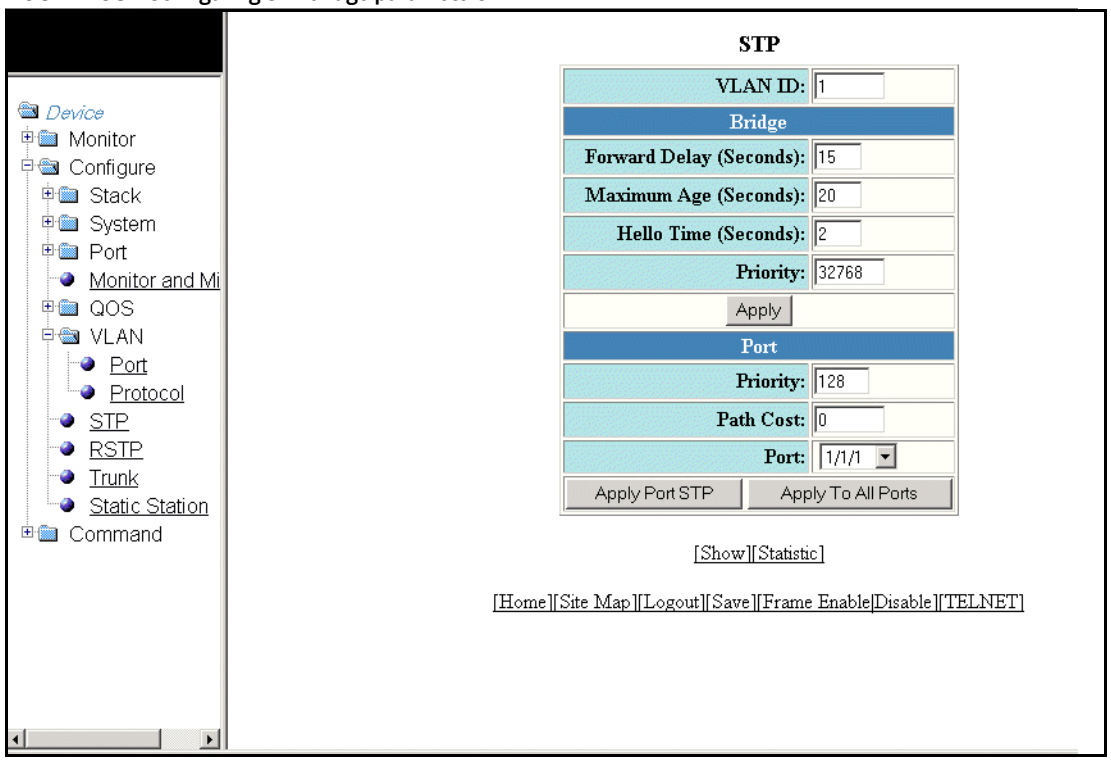
2. For Brocade FCX and Brocade ICX 6610 devices, select a unit ID in the **Select Stack Unit ID** list and click **Display** to display the information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available in the **STP Bridge** window for Brocade FSX devices.

3. To change the default values of the STP bridge, click **Modify**.

The **STP** window is displayed as shown in Figure 138.

FIGURE 138 Configuring STP bridge parameters



4. Type the VLAN identifier of the port in the **VLAN ID** field.

NOTE
The **VLAN ID** field is not available in the **STP** window for Brocade FSX devices.

5. Type the forward delay time, which is the period of time spent by a port in the listening and learning state before moving on to the learning or forwarding state, in the **Forward Delay (Seconds)** field. The range is from 4 through 30 seconds.
6. Type the maximum amount of time the device waits before a topology change in the **Maximum Age (Seconds)** field. The range is from 6 through 40 seconds.
7. Type the hello time, which is the interval of time between each configuration BPDU sent by the root bridge, in the **Hello Time (Seconds)** field. The range is from 1 through 10 seconds.
8. Type the priority used to identify the root bridge in a spanning tree in the **Priority** field. The range is from 0 through 65535.
9. Click **Apply**.

The message **The change has been made** is displayed and the configured values are displayed in the **STP Bridge** window. To display the **STP Bridge** window, click **Show**. To display STP information, click **Statistic**. For more information on the field descriptions, refer to "Displaying STP information" on page 51.

Changing STP port parameters

Table 53 lists the default STP port parameters.

TABLE 53 Default STP port parameters

Parameter	Default value
Priority	128
Path Cost	The default path cost depends on the port type. • 10 Mbps – 100 • 100 Mbps – 19 • 1 Gbps – 4 • 10 Gbps – 2

To change the default STP port values, perform the following steps.

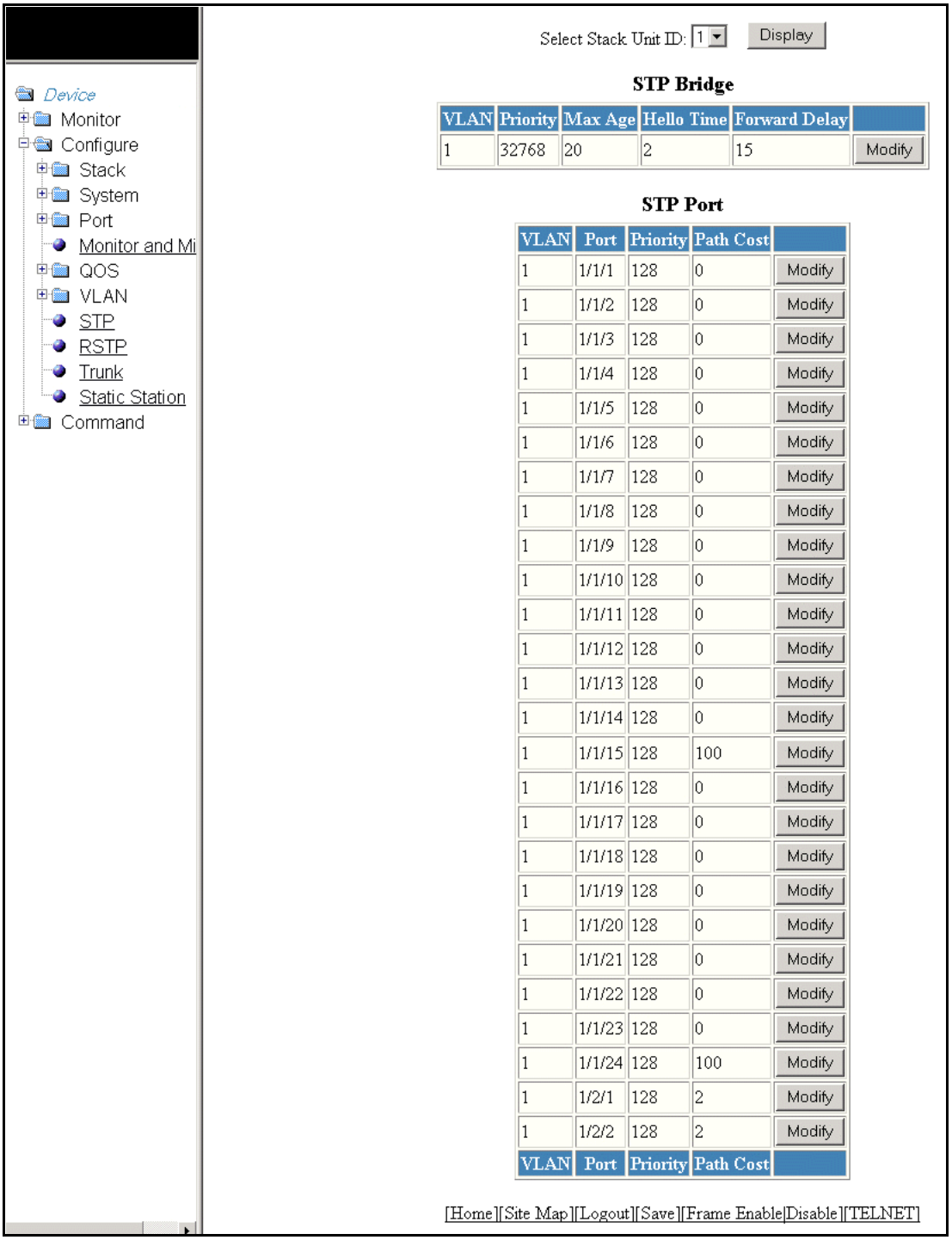
1. Click **Configure** on the left pane and select **STP**.

The **STP Port** window is displayed as shown in Figure 139.

2. For Brocade FCX and Brocade ICX 6610 devices, select a unit ID in the **Select Stack Unit ID** list and click **Display** to display the information about a specific stack unit.

NOTE
The **Select Stack Unit ID** list is not available in the **STP Bridge** window for Brocade FSX devices.

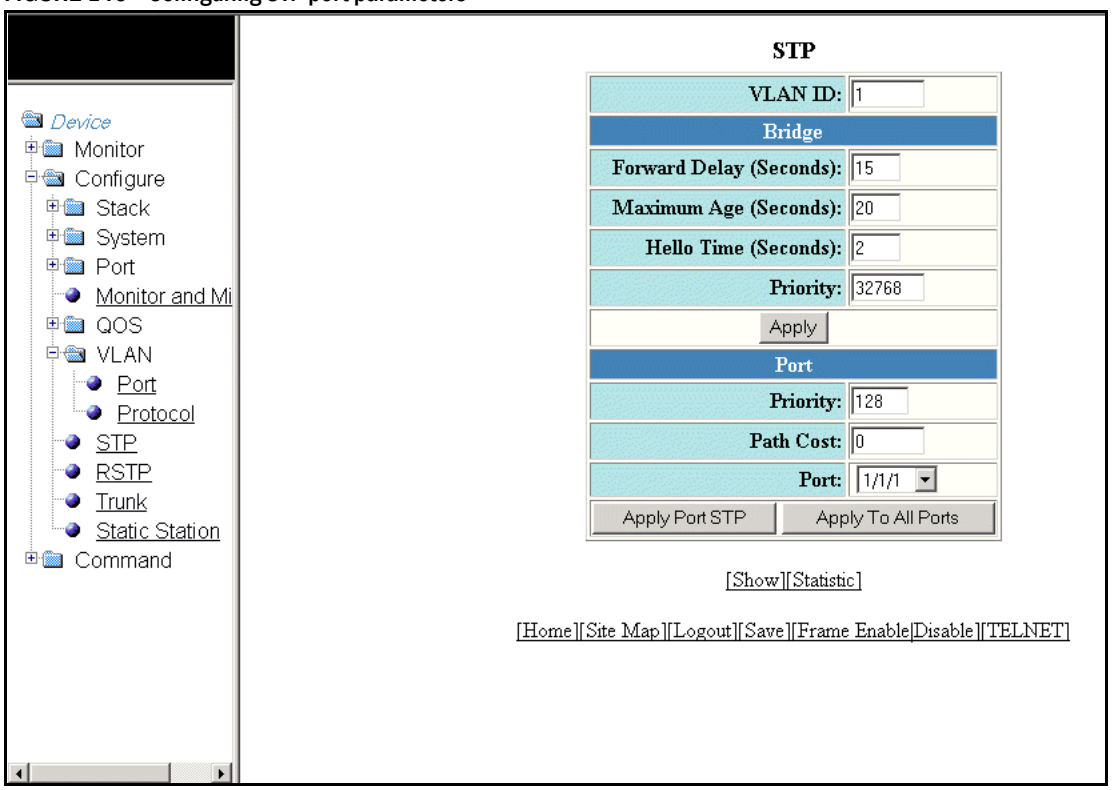
FIGURE 139 Configuring the STP port



3. Click **Modify** to change the default values of individual STP ports.

The **STP** window is displayed as shown in Figure 140.

FIGURE 140 Configuring STP port parameters



4. Type the VLAN identifier of the port in the **VLAN ID** field.
5. Type the preference that STP should give to this port relative to other ports for forwarding traffic out of the spanning tree in the **Priority** field. The range is from 0 through 240.
6. Type the cost of using the port to reach the root bridge in the **Path Cost** field. The range is from 0 through 65535.
7. Select a port number in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
8. Click **Apply Port STP** to configure the entered values only to the specified port. Click **Apply To All Ports** to configure the entered values to all the ports.

The message **The change has been made** is displayed and the configured values are displayed in the **STP Port** window. To display the **STP Port** window, click **Show**.

To display STP information, click **Statistic**. For more information on the field descriptions, refer to "Displaying STP information" on page 51.

Chapter

22

Configuring RSTP

In this chapter

- Configuring RSTP parameters. 207

Configuring RSTP parameters

You can change the RSTP default bridge and port parameters using the Web Management Interface.

Changing RSTP bridge parameters

Table 54 lists the default RSTP bridge parameters.

TABLE 54 Default RSTP bridge parameters

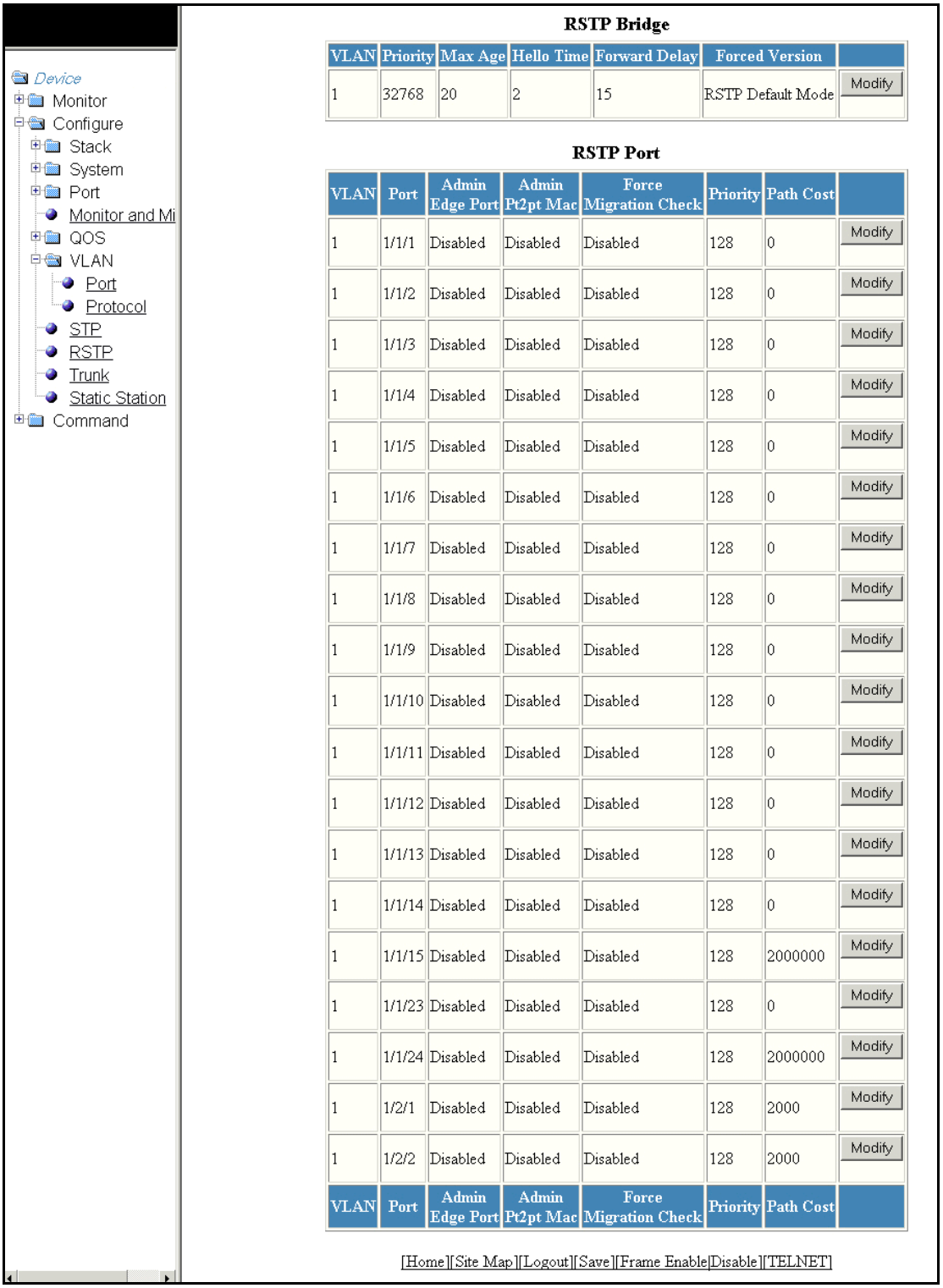
Parameter	Default value
Forward Delay	15 seconds
Maximum Age	20 seconds
Hello Time	2 seconds
Priority	32768
Force Version	RSTP Default Mode

To change the default RSTP bridge values, perform the following steps.

1. Click **Configure** on the left pane and select **RSTP**.

The **RSTP Bridge** window is displayed as shown in Figure 141.

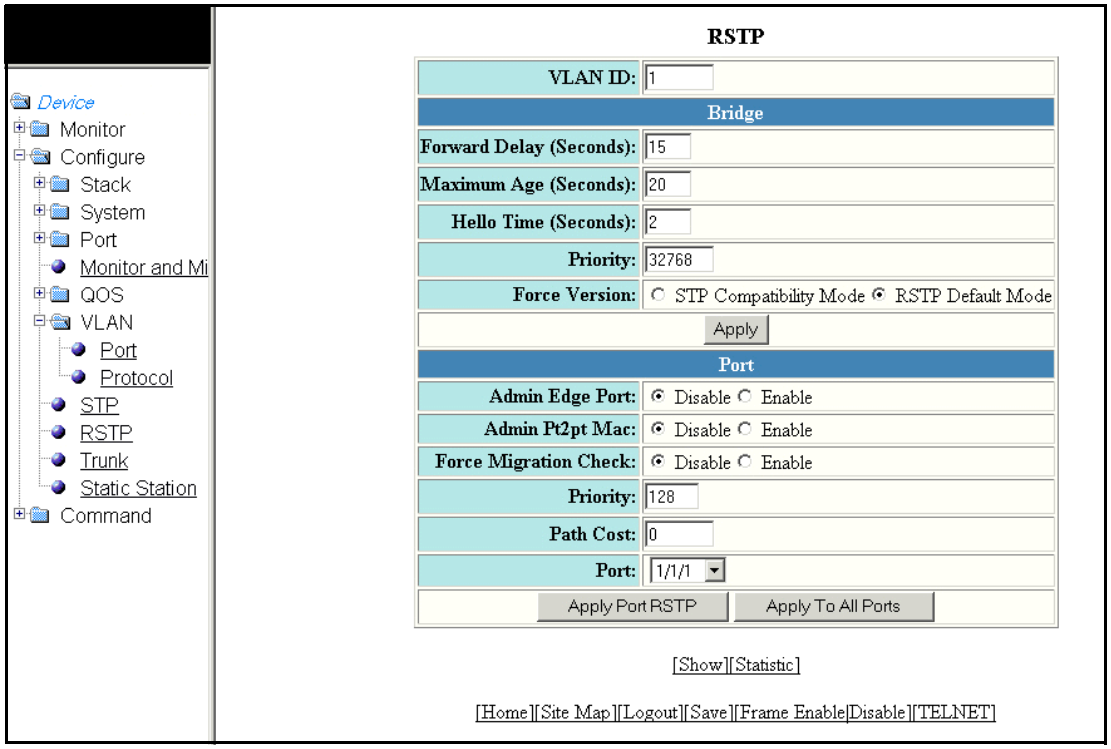
FIGURE 141 Configuring RSTP parameters


Device
Monitor
Configure
Stack
System
Port
Monitor and Mi
QOS
VLAN
Port
Protocol
STP
RSTP
Trunk
Static Station
Command
RSTP Bridge
VLAN Priority Max Age Hello Time Forward Delay Forced Version
1 32768 20 2 15 RSTP Default Mode Modify
RSTP Port
VLAN Port Admin Edge Port Admin Pt2pt Mac Force Migration Check Priority Path Cost
1 1/1/1 Disabled Disabled Disabled 128 0 Modify
1 1/1/2 Disabled Disabled Disabled 128 0 Modify
1 1/1/3 Disabled Disabled Disabled 128 0 Modify
1 1/1/4 Disabled Disabled Disabled 128 0 Modify
1 1/1/5 Disabled Disabled Disabled 128 0 Modify
1 1/1/6 Disabled Disabled Disabled 128 0 Modify
1 1/1/7 Disabled Disabled Disabled 128 0 Modify
1 1/1/8 Disabled Disabled Disabled 128 0 Modify
1 1/1/9 Disabled Disabled Disabled 128 0 Modify
1 1/1/10 Disabled Disabled Disabled 128 0 Modify
1 1/1/11 Disabled Disabled Disabled 128 0 Modify
1 1/1/12 Disabled Disabled Disabled 128 0 Modify
1 1/1/13 Disabled Disabled Disabled 128 0 Modify
1 1/1/14 Disabled Disabled Disabled 128 0 Modify
1 1/1/15 Disabled Disabled Disabled 128 2000000 Modify
1 1/1/23 Disabled Disabled Disabled 128 0 Modify
1 1/1/24 Disabled Disabled Disabled 128 2000000 Modify
1 1/2/1 Disabled Disabled Disabled 128 2000 Modify
1 1/2/2 Disabled Disabled Disabled 128 2000 Modify
VLAN Port Admin Edge Port Admin Pt2pt Mac Force Migration Check Priority Path Cost
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

2. Click **Modify**.

The **RSTP** window is displayed as shown in Figure 142.

FIGURE 142 Changing RSTP bridge values



3. Type the forward delay, which specifies how long a port waits before it forwards an RST BPDU after a topology change, in the **Forward Delay (Seconds)** field. The range is from 4 through 30 seconds.
4. Type the maximum age, which specifies the amount of time the device waits to receive a hello packet before it starts a topology change, in the **Maximum Age (Seconds)** field. The range is from 6 through 40 seconds.
5. Type the hello time, which specifies the interval between two hello packets, in the **Hello Time (Seconds)** field. The range is from 1 through 10 seconds.
6. Type the priority of the bridge in the **Priority** field. The range is from 0 through 65535.
7. Click **STP Compatibility Mode** or **RSTP Default Mode** for **Force Version**. By default, **RSTP Default Mode** is enabled.
8. Click **Apply**.

The message **The change has been made** is displayed and the configured values are shown in the **RSTP Bridge** window.

Changing RSTP port parameters

Table 55 lists the default RSTP port parameters.

TABLE 55 Default RSTP port parameters

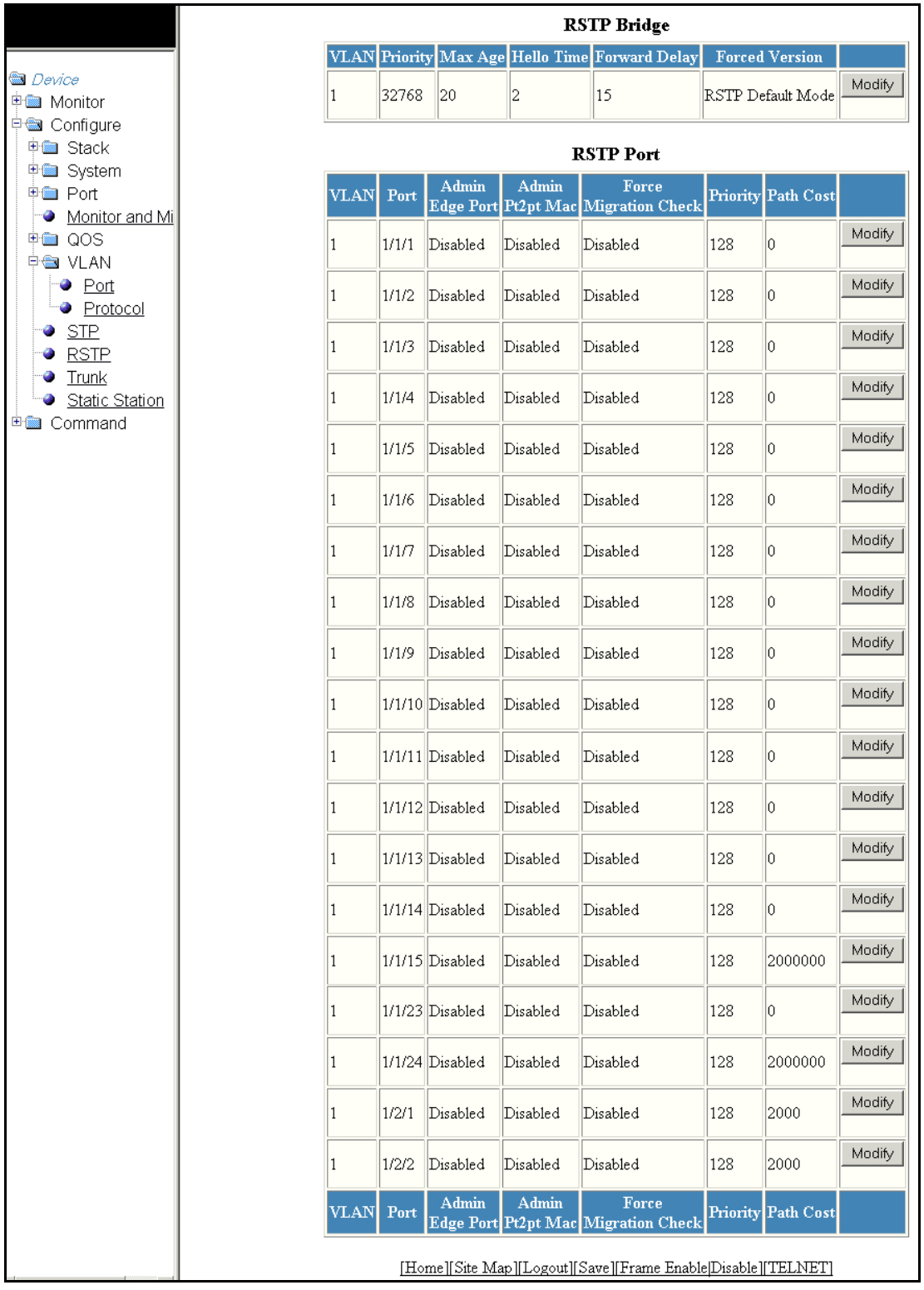
Parameter	Default value
Admin Edge Port	Disable
Admin Pt2pt Mac	Disable
Force Migration Check	Disable
Priority	128
Path Cost	The default path cost varies based on the products: • For Brocade FCX and Brocade ICX 6610 devices - 0 • For FSX devices - 2000

To change the default RSTP port values, perform the following steps.

1. Click **Configure** on the left pane and select **RSTP**.

The **RSTP Port** window is displayed as shown in Figure 143.

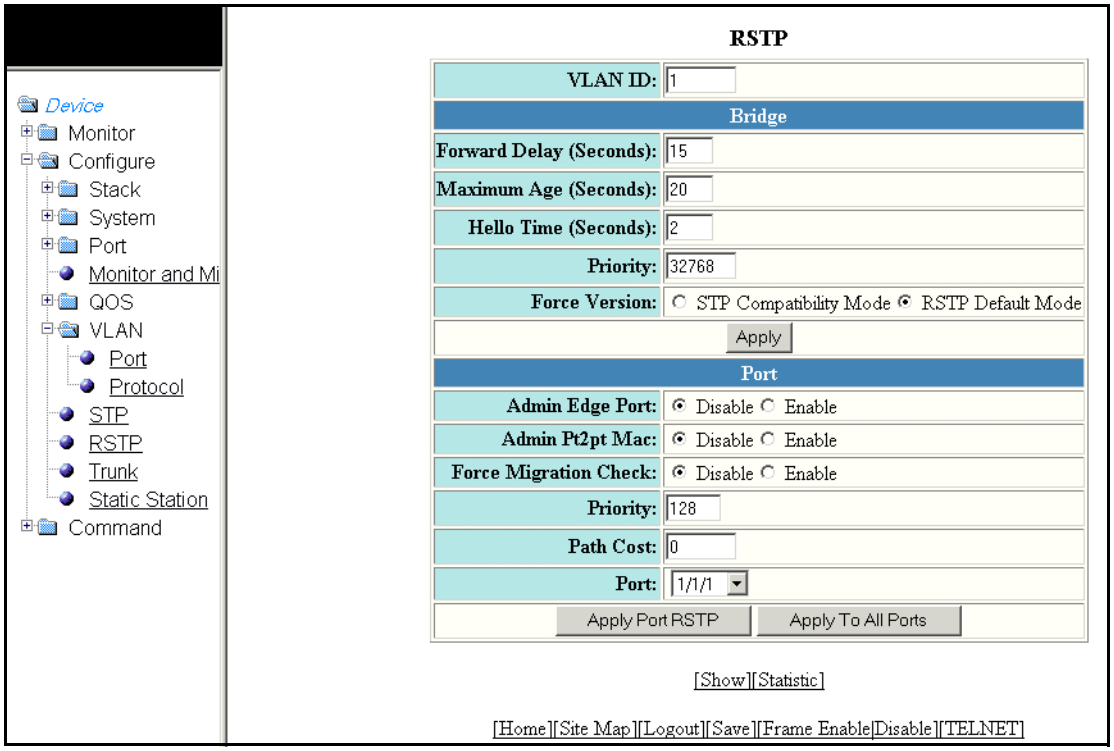
FIGURE 143 Configuring RSTP ports


Device
Monitor
Configure
Stack
System
Port
Monitor and Mi
QOS
VLAN
Port
Protocol
STP
RSTP
Trunk
Static Station
Command
RSTP Bridge
VLAN Priority Max Age Hello Time Forward Delay Forced Version
1 32768 20 2 15 RSTP Default Mode Modify
RSTP Port
VLAN Port Admin Edge Port Admin Pt2pt Mac Force Migration Check Priority Path Cost
1 1/1/1 Disabled Disabled Disabled 128 0 Modify
1 1/1/2 Disabled Disabled Disabled 128 0 Modify
1 1/1/3 Disabled Disabled Disabled 128 0 Modify
1 1/1/4 Disabled Disabled Disabled 128 0 Modify
1 1/1/5 Disabled Disabled Disabled 128 0 Modify
1 1/1/6 Disabled Disabled Disabled 128 0 Modify
1 1/1/7 Disabled Disabled Disabled 128 0 Modify
1 1/1/8 Disabled Disabled Disabled 128 0 Modify
1 1/1/9 Disabled Disabled Disabled 128 0 Modify
1 1/1/10 Disabled Disabled Disabled 128 0 Modify
1 1/1/11 Disabled Disabled Disabled 128 0 Modify
1 1/1/12 Disabled Disabled Disabled 128 0 Modify
1 1/1/13 Disabled Disabled Disabled 128 0 Modify
1 1/1/14 Disabled Disabled Disabled 128 0 Modify
1 1/1/15 Disabled Disabled Disabled 128 2000000 Modify
1 1/1/23 Disabled Disabled Disabled 128 0 Modify
1 1/1/24 Disabled Disabled Disabled 128 2000000 Modify
1 1/2/1 Disabled Disabled Disabled 128 2000 Modify
1 1/2/2 Disabled Disabled Disabled 128 2000 Modify
VLAN Port Admin Edge Port Admin Pt2pt Mac Force Migration Check Priority Path Cost
[Home][Site Map][Logout][Save][Frame Enable|Disable][TELNET]

2. Click **Modify** to change the default values for an individual RSTP port.

The **RSTP** window is displayed as shown in Figure 144.

FIGURE 144 Changing RSTP port values



3. Click **Disable** or **Enable** for **Admin Edge Port**. If you click **Enable**, the port becomes an edge port in the domain.
4. Click **Disable** or **Enable** for **Admin Pt2pt Mac**. If you click **Enable**, a port will be connected to another port through a point-to-point link.
5. Click **Disable** or **Enable** for **Force Migration Check**. If you click **Enable**, the specified port will be forced to send one RST BPDU. If only STP BPDUs are received in response to the sent RST BPDU, then the port returns to sending STP BPDUs.
6. Type the priority, which is the preference that RSTP gives to this port relative to other ports for forwarding traffic out of the topology, in the **Priority** field. The range is from 0 through 240.
7. Type the cost of the port path to the root bridge in the **Path Cost** field. The range is from 1 through 20,000,000.
8. Select a port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
9. Click **Apply Port RSTP** to configure the values only to the specified port, or click **Apply To All Ports** to configure the values to all the ports.

The message **The change is made is displayed** and the configured RSTP port values are reflected in the **RSTP Port** window.

Chapter

23

Configuring Trunks

In this chapter

- Adding trunks 213

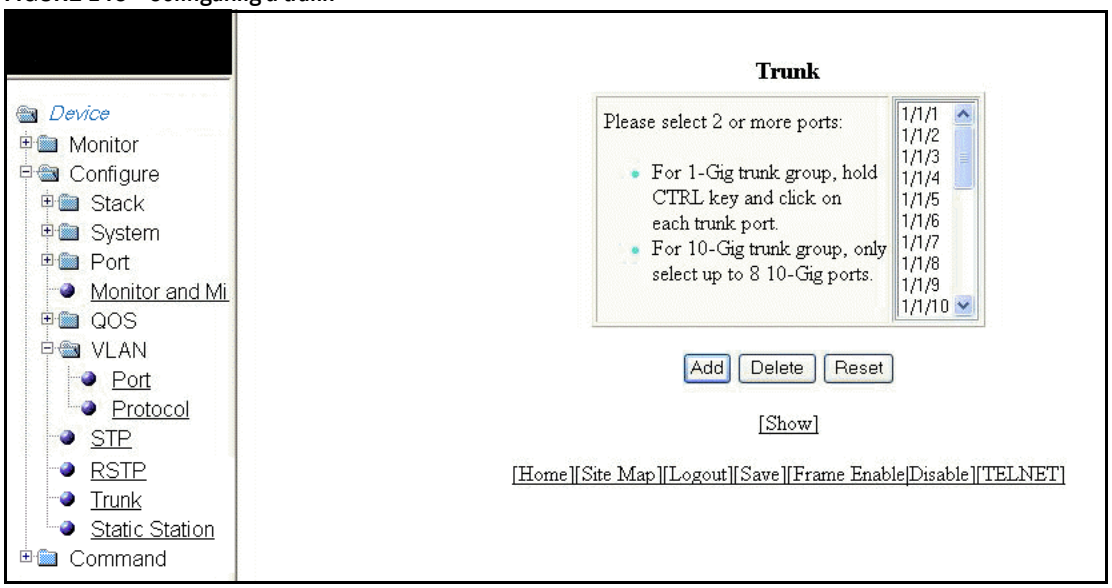
Adding trunks

To configure a trunk, perform the following steps.

1. Click **Configure** on the left pane and select **Trunk**.

The **Trunk** window is displayed as shown in Figure 145.

FIGURE 145 Configuring a trunk



2. Hold **CTRL** on your keyboard and select the ports that you want to add in a trunk group.

NOTE
The port number varies based on the product:

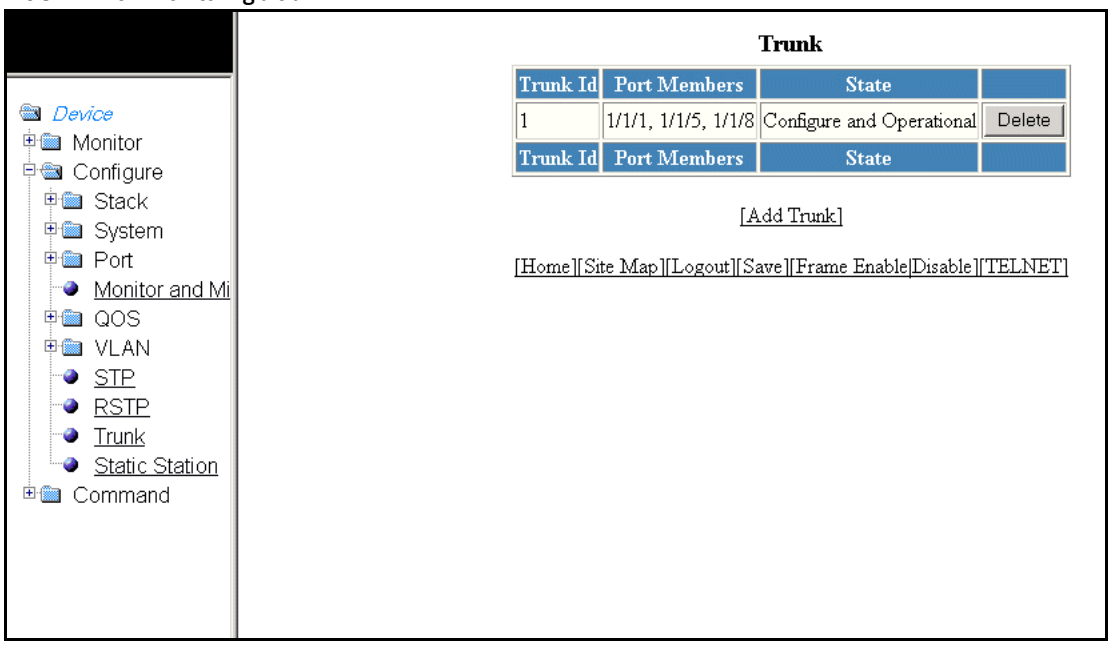
- For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
- For Brocade FSX devices – slotnum/portnum

3. Click **Add**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**. You can also delete the trunk group by clicking **Delete**.

To display the configured trunk group, click **Show**. Figure 146 shows the **Trunk** window with the configured trunk information.

FIGURE 146 Monitoring a trunk



Chapter

24

Configuring a Static Station

In this chapter

- Adding a static station 215
- Modifying a static station 216

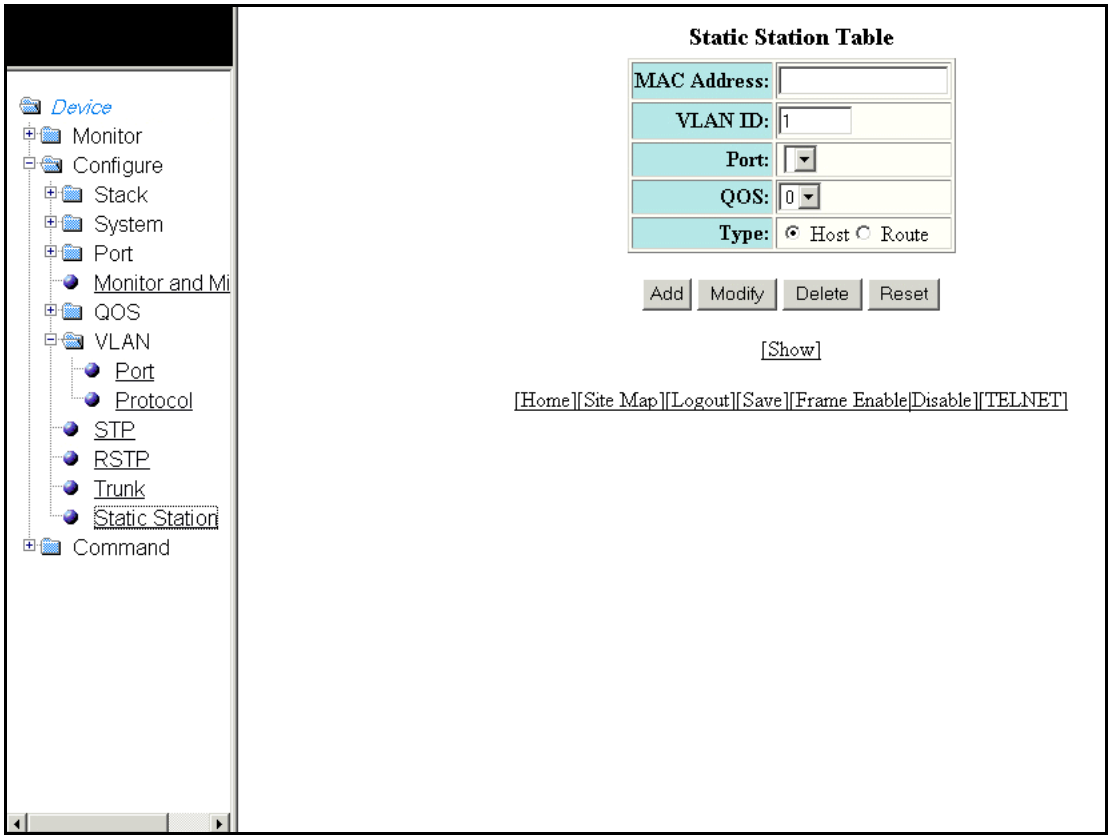
Adding a static station

To configure a static MAC entry and assign the traffic priority (QoS) and VLAN membership (VLAN ID) to the entry, perform the following steps.

1. Click **Configure** on the left pane and select **Static Station**.

The **Static Station Table** window is displayed as shown in Figure 147.

FIGURE 147 Configuring the static station



2. Type the MAC address of the device in xx-xx-xx-xx-xx-xx format in the **MAC Address** field.

3. Type the port-based VLAN identifier in the **VLAN ID** field. VLAN 1 is the default VLAN.
4. Select a port number in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
5. Select a QoS priority in the **QOS** list. A static MAC entry can be assigned a priority from 0 through 7.
6. Click **Host** or **Route** for **Type**. By default, **Host** is selected.
7. Click **Add**.

The message **The change has been made** is displayed. To display the configured static station, click **Show.**

To reset the data entered in the configuration pane, click **Reset**. You can also delete the configured static station entry by clicking **Delete**.

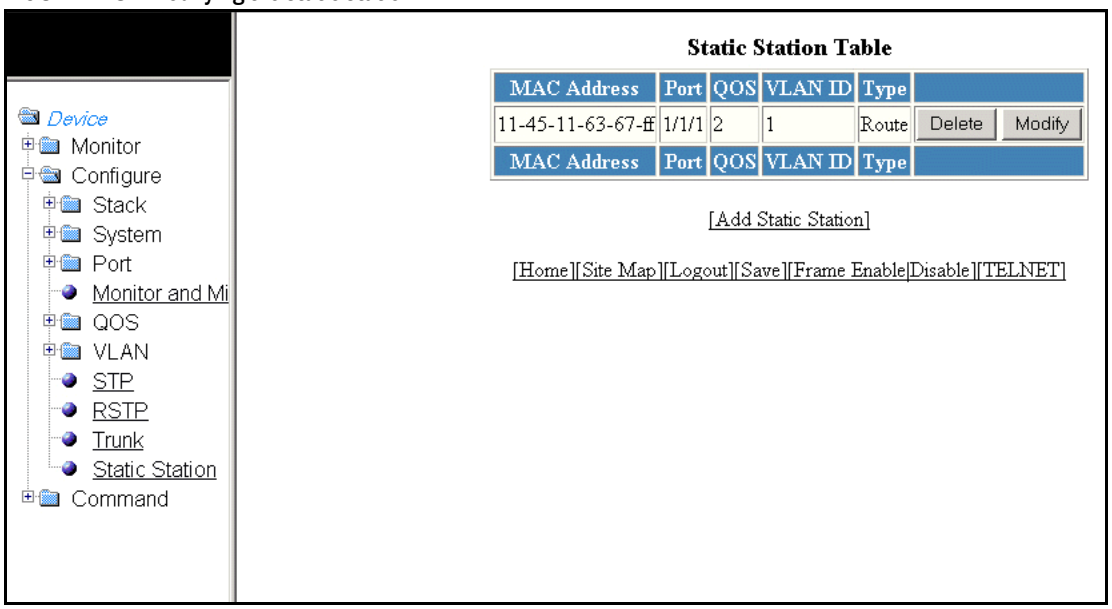
Modifying a static station

After you configure a static station, you can modify the port number, QoS priority, VLAN ID, and device type of the entry by performing the following steps.

1. Click **Configure** on the left pane and select **Static Station**.

The **Static Station Table** window is displayed as shown in Figure 148.

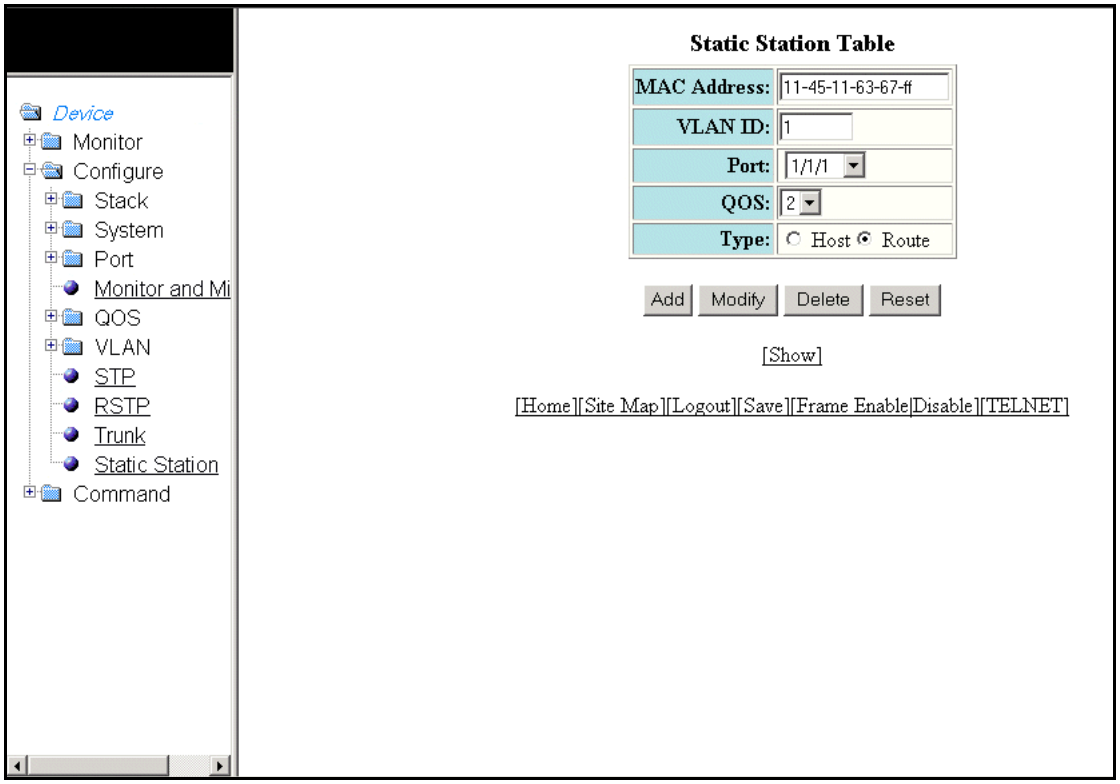
FIGURE 148 Modifying the static station



2. Click **Modify**.

The **Static Station Table** window is displayed as shown in Figure 149.

FIGURE 149 Modifying the static station



3. Type the port-based VLAN identifier in the **VLAN ID** field. VLAN 1 is the default VLAN.

NOTE
The **VLAN ID** field is not available in the **Static Station Table** window for Brocade FSX devices.

4. Select a port number in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
5. Select a QoS priority in the **QOS** list. A static MAC entry can be assigned a priority from 0 through 7.
6. Click **Host** or **Route** for **Type**.
7. Click **Modify**.

The message **The change has been made** is displayed and the configured values are reflected in the **Static Station** window. To display the modified static station, click **Show**.

To reset the data entered in the configuration pane, click **Reset**. You can also delete the static station entry by clicking **Delete**.

Chapter

25

Configuring IP

In this chapter

- Configuring the router IP address. 219
- Configuring a standard ACL 220
- Configuring an extended ACL 222
- Configuring an IP access group 224
- Configuring an IP AS-path access list. 225
- Configuring an IP community list 226
- Configuring an IP prefix list. 228
- Configuring a DNS entry 229
- Configuring the general IP settings 230
- Configuring IP interfaces. 231
- Configuring a static ARP 232
- Configuring a static RARP 233
- Configuring a static route 234
- Configuring a UDP helper 236

NOTE
The IP feature is specific to Brocade FCX, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

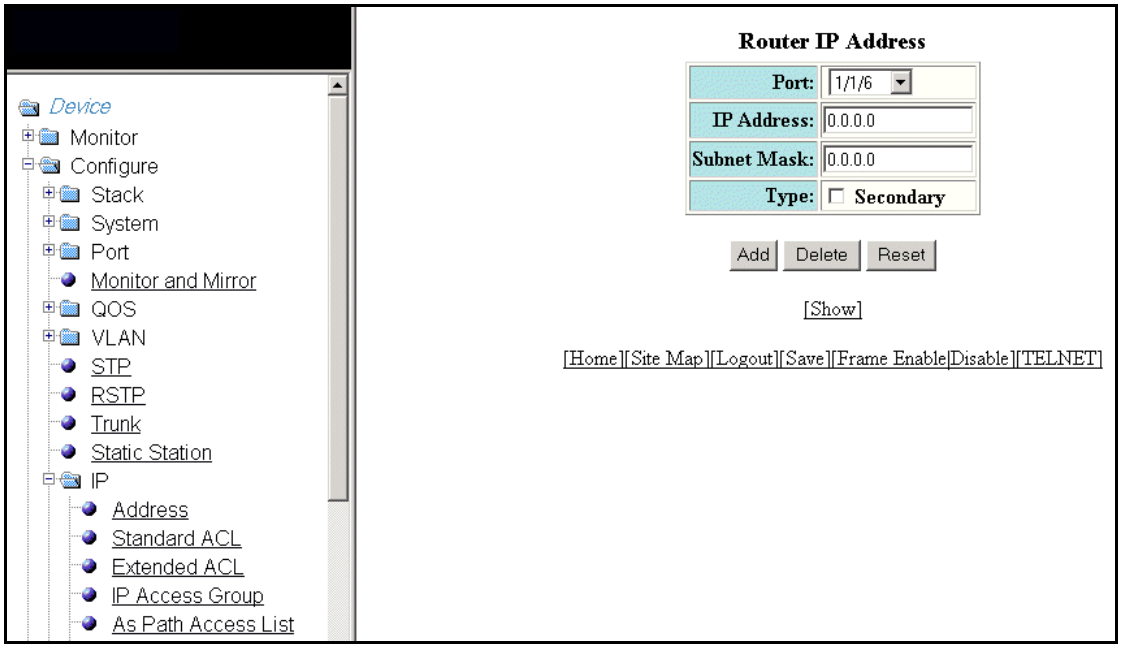
Configuring the router IP address

To configure an IP address to an interface, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Address**.

The **Router IP Address** window is displayed as shown in Figure 150.

FIGURE 150 Configuring router IP addresses



3. Select a port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Type the IP address of the device in the **IP Address** field.
5. Type the IP subnet mask in the **Subnet Mask** field.
6. Select the **Secondary** check box for **Type** if you have already configured an IP address within the same subnet on the interface.
7. Click **Add**.

The message **The change has been made** is displayed and the specified IP address is assigned to the interface. To display the configured router IP address, click **Show**.

To delete the configured IP address, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

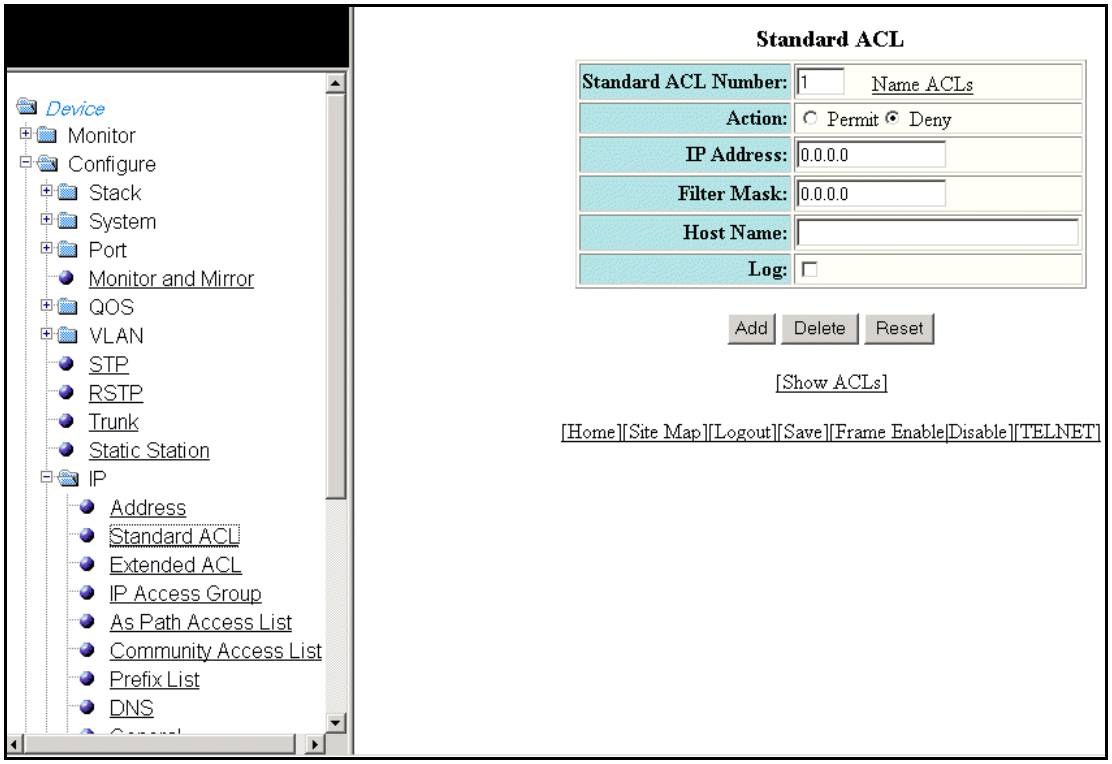
Configuring a standard ACL

To configure a standard ACL, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Standard ACL**.

The **Standard ACL** window is displayed as shown in Figure 151.

FIGURE 151 Configuring standard ACLs



3. Type the ACL number from 1 through 99 in the **Standard ACL Number** field. If you want to type an ACL name, click **Name ACLs**. The field label changes to **Standard ACL Name**. Now you can type an ACL name up to 256 alphanumeric characters in length.
4. Click **Permit** or **Deny** for **Action** so that the packets that match a policy in the ACL can be permitted (forwarded) or denied (dropped).
5. Type the host IP address in the **IP Address** field.
6. Type the IP subnet mask in the **Filter Mask** field.
7. Type the host name in the **Host Name** field.
8. Select the **Log** check box so that the device generates syslog entries and SNMP traps for the packets that are denied by the access policy.
9. Click **Add**.

The message **The change has been made** is displayed and the ACL is added. To display the configured ACL, click **Show ACLs**.

To delete the configured ACL, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

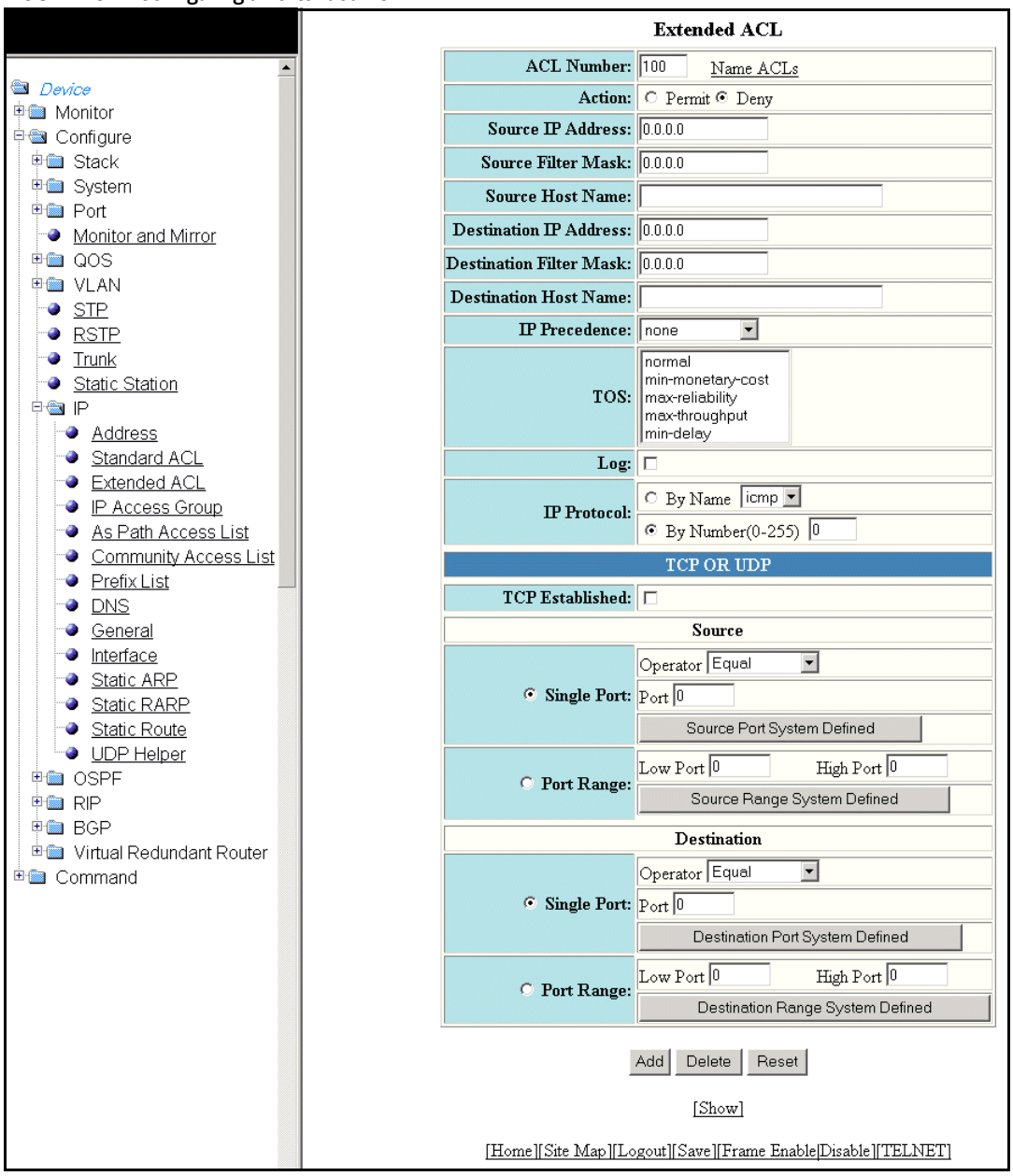
Configuring an extended ACL

To configure an extended numbered ACL, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Extended ACL**.

The **Extended ACL** window is displayed as shown in Figure 152.

FIGURE 152 Configuring an extended ACL



3. Type the extended ACL number from 100 through 199 in the **ACL Number** field. If you want to specify the extended ACL name, click **Name ACLs**. The field label is changed to **ACL Name**.

4. Click **Permit** or **Deny** for **Action** so that the packets that match the policy can be forwarded or dropped.
5. Type the source IP address in the **Source IP Address** field.
6. Type the source mask in the **Source Filter Mask** field.
7. Type the source host name in the **Source Host Name** field.
8. Type the destination IP address in the **Destination IP Address** field.
9. Type the destination mask in the **Destination Filter Mask** field.
10. Type the destination host name in the **Destination Host Name** field.
11. Select one of the following options in the **IP Precedence** list:
    - **routine** – The ACL matches packets that have the routine precedence.
    - **priority** – The ACL matches packets that have the priority precedence.
    - **immediate** – The ACL matches packets that have the immediate precedence.
    - **flash** – The ACL matches packets that have the flash precedence.
    - **flash-override** – The ACL matches packets that have the flash override precedence.
    - **critical** – The ACL matches packets that have the critical precedence.
    - **internet** – The ACL matches packets that have the internetwork control precedence.
    - **network** – The ACL matches packets that have the network control precedence.
12. Select one of the following options in the **TOS** list:
    - **normal** – The ACL matches packets that have the normal ToS.
    - **min-monetary-cost** – The ACL matches packets that have the minimum monetary cost ToS.
    - **max-reliability** – The ACL matches packets that have the maximum reliability ToS.
    - **max-throughput** – The ACL matches packets that have the maximum throughput ToS.
    - **min-delay** – The ACL matches packets that have the minimum delay ToS.
13. Select the **Log** check box to enable generation of SNMP traps and syslog messages for packets denied by the ACL.
14. Click **By Name** for **IP Protocol** to select the IP protocol by name or click **By Number** to specify the number (from 0 through 255).
15. Select the **TCP Established** check box so that the policy applies to the TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to “1”) in the Control Bits field of the TCP packet header. The policy applies only to the established TCP sessions, not to the new sessions.

NOTE
This field applies only to the destination TCP ports, not the source TCP ports.

16. Enter the following information for **Source**:
    a. To configure a single port, click **Single Port**.
        i. Select one of the following for **Operator**:
        - **Equal** - The policy applies to the TCP or UDP port name or number you enter.
        - **NotEqual** - The policy applies to all the TCP or UDP port numbers except the port number or port name you enter.
        - **LessThan** - The policy applies to the TCP or UDP port numbers that are less than the port number or the numeric equivalent to the port name you enter.
        - **GreaterThan** - The policy applies to the TCP or UDP port numbers greater than the port number or the numeric equivalent to the port name you enter.

        ii. Click **Source Port System Defined**.
    b. To configure a range of ports, click **Port Range**.
        i. Type the lower port number in the **Low Port** field and the highest port number in the **High Port** field.
        ii. Click **Source Range System Defined**.
17. To configure the destination port settings under **Destination**, follow the procedure explained in step 16.
18. Click **Add**.

The message **The change has been made** is displayed. To display the configured extended numbered ACL, click **Show**.

To delete the configured extended numbered ACL, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

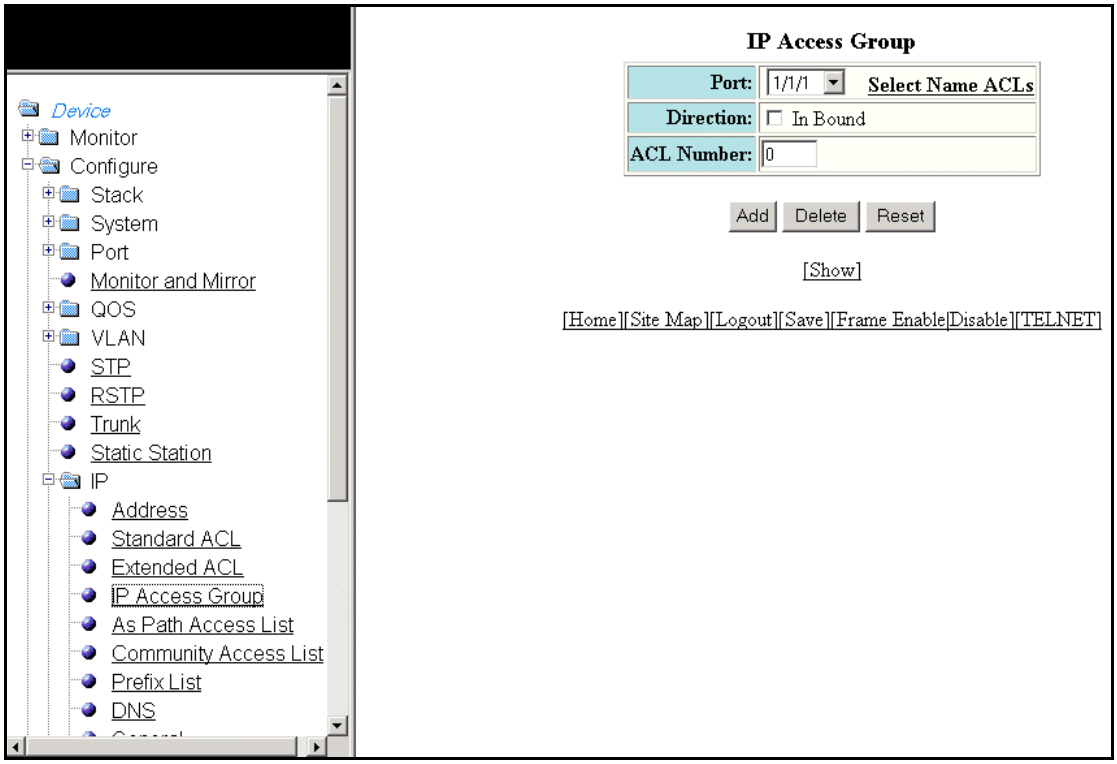
Configuring an IP access group

To configure an IP access group, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **IP Access Group**.

The **IP Access Group** window is displayed as shown in Figure 153.

FIGURE 153 Configuring IP access groups



3. Select a port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Select the **In Bound** check box for **Direction** to enable incoming traffic on the interface to which you apply the ACL.
5. Type the ACL number in the **ACL Number** field. If you want to type an ACL name, click **Select Name ACLs**. The field label changes to **ACL Name**. Now you can type the ACL name up to 256 alphanumeric characters in length.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured IP access group, click **Show**.

To delete the configured IP access group, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

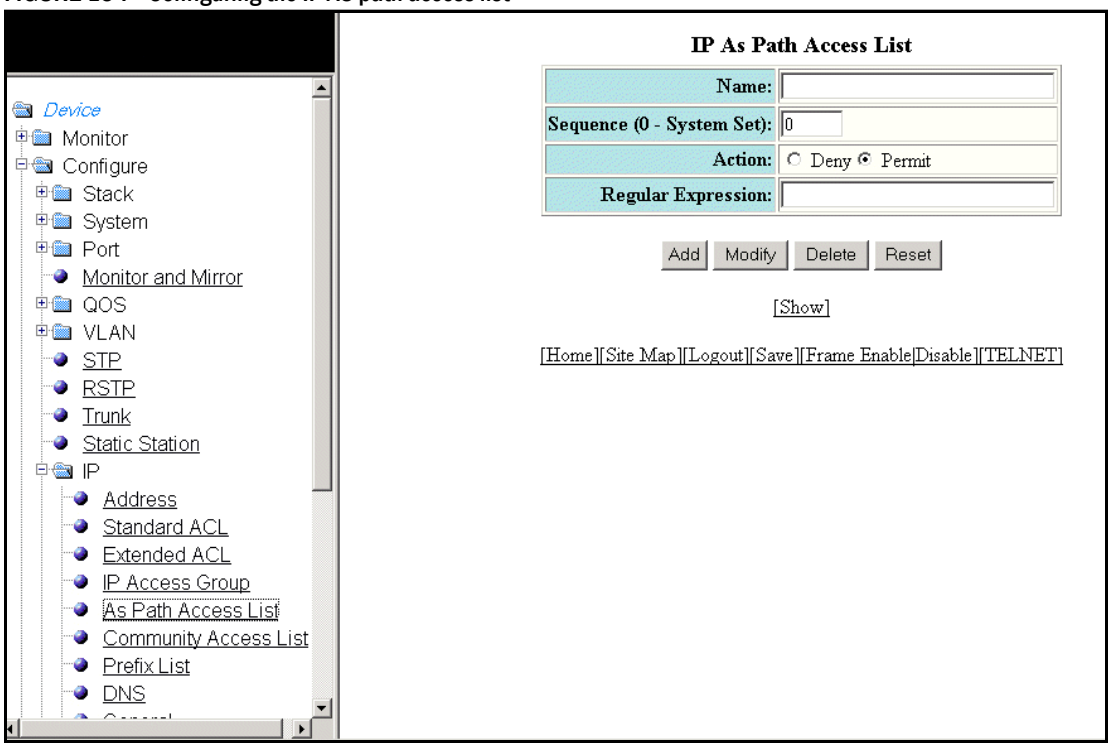
Configuring an IP AS-path access list

To configure an AS-path access list, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **As Path Access List**.

The **IP As Path Access List** window is displayed as shown in Figure 154.

FIGURE 154 Configuring the IP AS path access list



3. Type the ACL name in the **Name** field.
4. Type the AS-path list sequence number in the **Sequence (0 - System Set)** field. You can configure up through 199 entries in an AS-path list.

   If you do not specify a sequence number, the software entries them in increments of five, beginning with number five. The software interprets the entries in an AS-path list in numerical order, beginning with the lowest sequence number.
5. Click **Deny** or **Permit** for **Action**.
6. Type the AS-path information you want to permit or deny to routes that match any of the match statements within the ACL in the **Regular Expression** field.
7. Click **Add**.

The message **The change has been made** is displayed. To display the configured AS-path list, click **Show**.

To modify the AS-path list, click **Modify**. You can also delete the AS-path list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

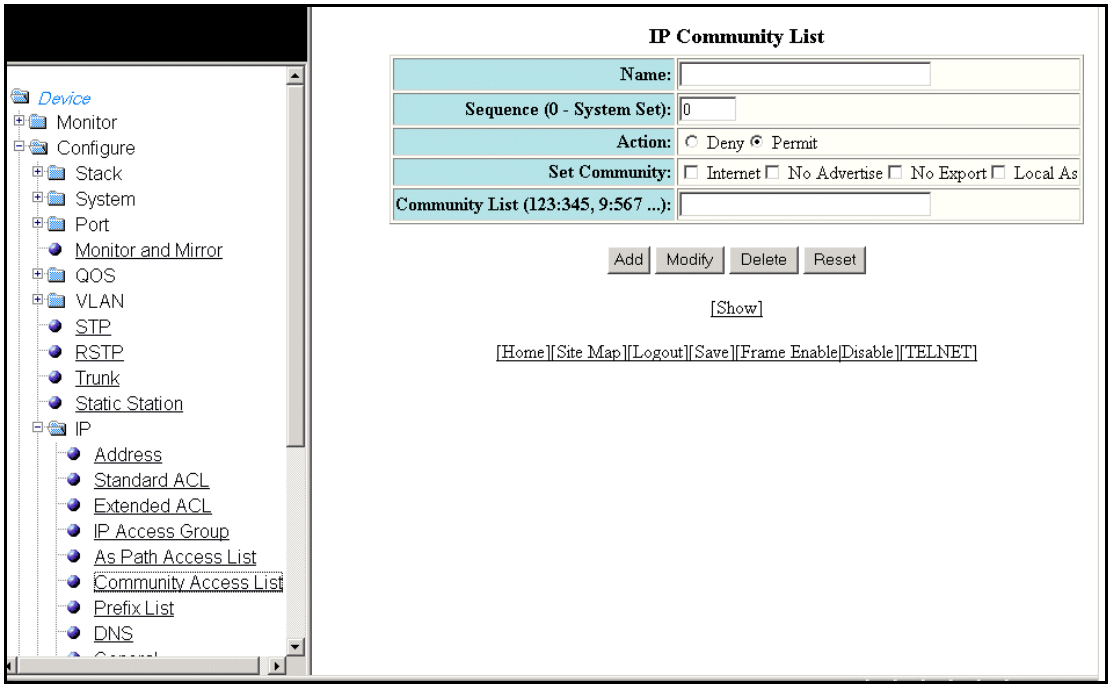
Configuring an IP community list

To configure an IP community list, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Community Access List**.

The **IP Community List** window is displayed as shown in Figure 155.

FIGURE 155 Configuring the IP community list



3. Type the ACL name in the **Name** field.
4. Type the community list sequence number in the **Sequence (0 - System Set)** field. You can configure up to 199 entries in a community list.

   If you do not specify a sequence number, the software numbers entries in increments of five, beginning with number five. The software interprets the entries in a community list in numerical order, beginning with the lowest sequence number.
5. Click **Deny** or **Permit** for **Action**.
6. Select one of the following options for **Set Community**:
   - **Internet** – The Internet community.
   - **No Advertise** – Routes with this community cannot be advertised to any other BGP Layer 3 switches.
   - **No Export** – The community of sub-Autonomous Systems (AS) within a confederation. Routes with this community can be exported to other sub-ASes within the same confederation but cannot be exported outside the confederation to other ASes or otherwise sent to EBGP neighbors.
   - **Local As** – The local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.
7. Type the community number in *num*:*num* format in the **Community List** field.
8. Click **Add**.

The message **The change has been made** is displayed. To display the configured community list, click **Show**.

To modify the community list, click **Modify**. You can also delete the community list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

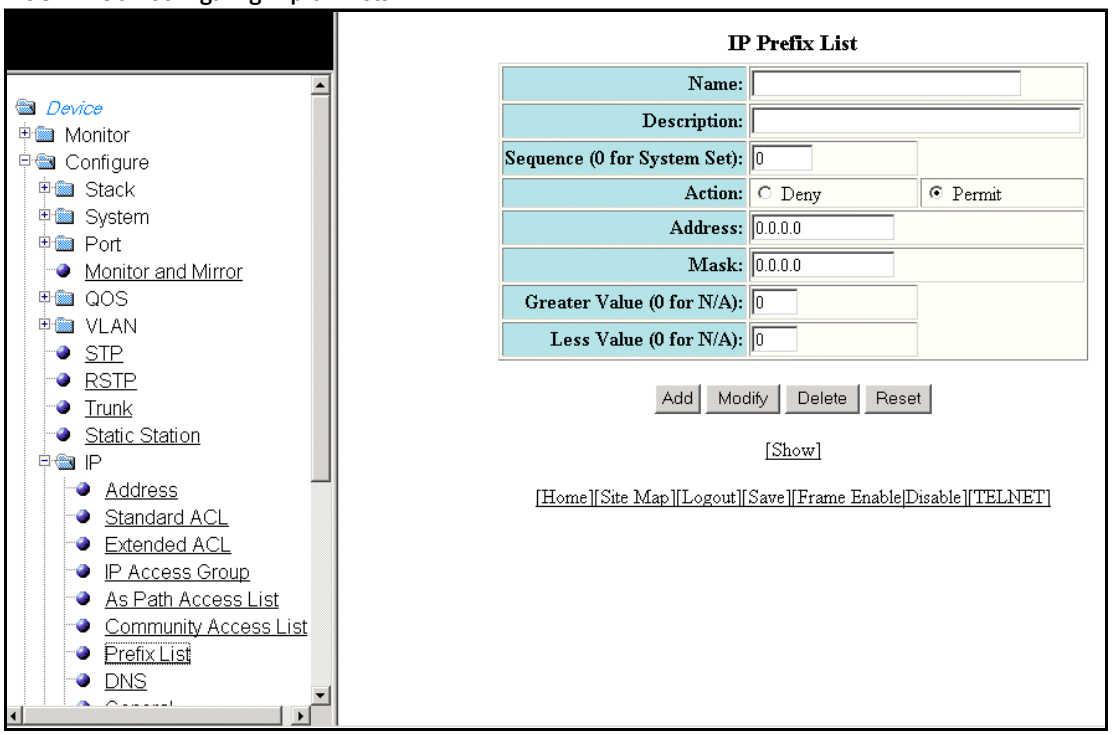
Configuring an IP prefix list

To configure an IP prefix list, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Prefix List**.

The **IP Prefix List** window is displayed as shown in Figure 156.

FIGURE 156 Configuring IP prefix lists



3. Type the prefix list name in the **Name** field.
4. Type a text string describing the prefix list in the **Description** field.
5. Type the IP prefix list sequence number in the **Sequence (0 for System Set)** field. You can configure up to 100 prefix list entries.

   If you do not specify a sequence number, the software numbers entries in increments of five, beginning with prefix list entry five. The software interprets the prefix list entries in numerical order, beginning with the lowest sequence number.
6. Click **Deny** or **Permit** for **Action**.
7. Type the network IP address in the **Address** field.
8. Type the network mask address in the **Mask** field.
9. Type the maximum value of the mask length in the **Greater Value (0 for N/A)** field.
10. Type the least value of the mask length in the **Less Value (0 for N/A)** field.

NOTE
The **Greater Value (0 for N/A)** or **Less Value (0 for N/A)** values you specify must meet the following condition:
Length < Greater Value <= Less Value <= 32

11. Click **Add**.

The message **The change has been made** is displayed. To display the configured IP prefix list, click **Show**.

To modify the IP prefix list, click **Modify**. You can also delete the IP prefix list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a DNS entry

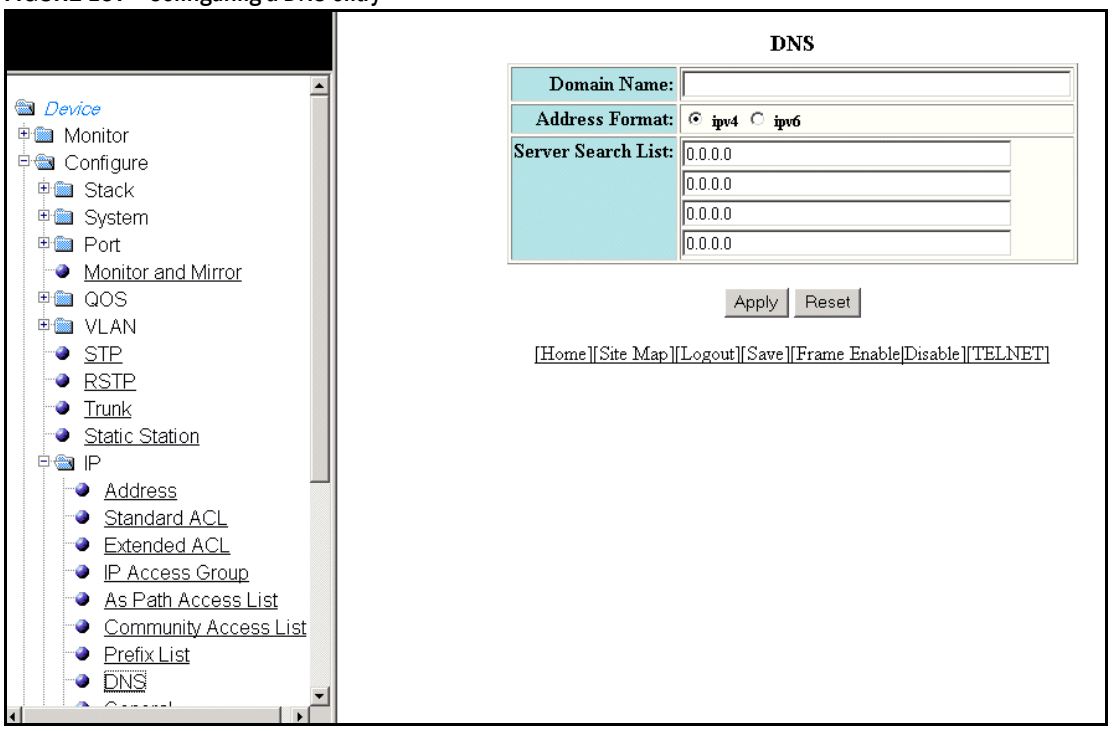
You can configure the Brocade device to recognize up to four Domain Name System (DNS) servers. The first entry serves as the primary default address. If a query to the primary address fails to be resolved after three attempts, the next DNS address is queried (also up to three times). This process continues for each defined DNS address until the query is resolved. The order in which the default DNS addresses are polled is the same as the order in which you enter them.

To configure DNS, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **DNS**.

The **DNS** window is displayed as shown in Figure 157.

FIGURE 157 Configuring a DNS entry



3. Type the domain name in the **Domain Name** field.
4. Click **ipv4** or **ipv6** for **Address Format**.
5. Type the IPv4 or IPv6 address of the DNS in the **Server Search List** fields.
6. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

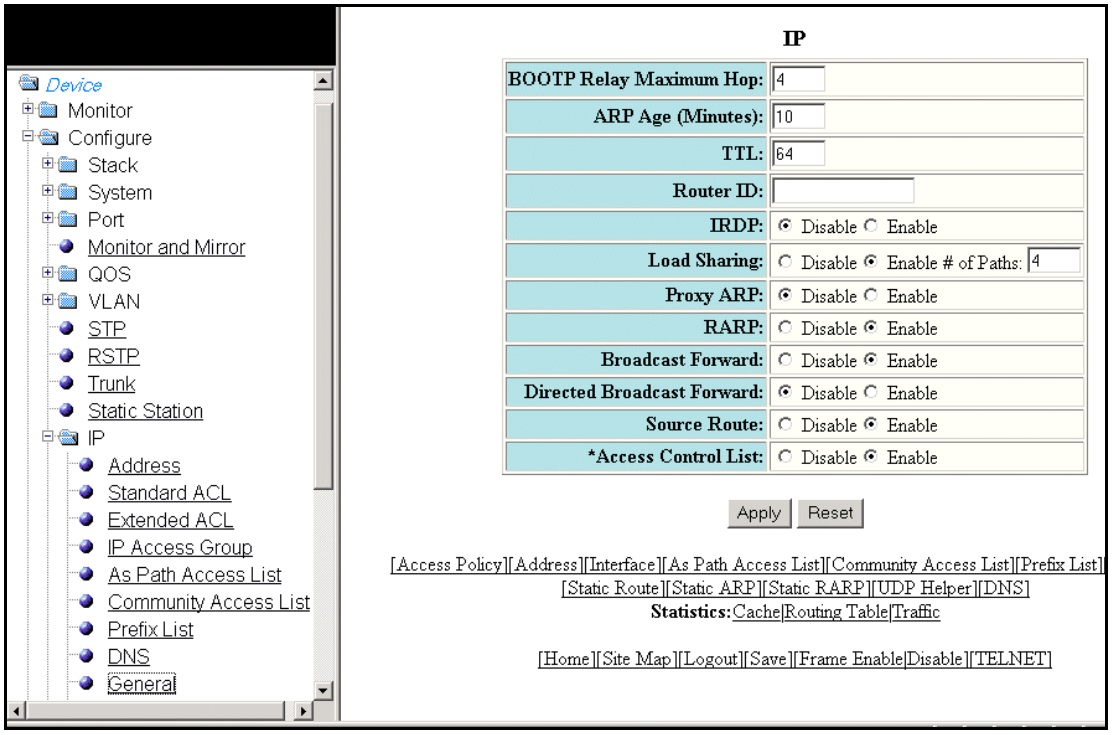
Configuring the general IP settings

To configure the general IP settings, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **General**.

The **IP** window is displayed as shown in Figure 158.

FIGURE 158 Configuring the general IP settings



3. Type the maximum number of hops away a BootP server can be located from a Layer 3 switch and still be used by the router clients for network booting in the **BOOTP Relay Maximum Hop** field. The range is from 1 through 15. The default value is four.
4. Type the amount of time the device should keep a MAC address learned through ARP in the device ARP cache in the **ARP Age (Minutes)** field. The range is 0 through 240 minutes. The default is 10 minutes.
5. Type the maximum number of Layer 3 switches (hops) through which a packet can pass before being discarded in the **TTL** field. The range is from 1 through 255 hops. The default is 64 hops.

6. Type the Layer 3 switch identifier in the **Router ID** field.
7. Click **Disable** or **Enable** for **IRDP**. By default, this protocol is disabled.

   ICMP Router Discovery Protocol (IRDP) is an IP protocol a Layer 3 switch can use to advertise the IP addresses of its interfaces to the directly attached hosts.
8. Click **Disable** or **Enable** for **Load Sharing**. If you click **Enable**, type the number of load sharing paths in the **# of Paths** field.
9. Click **Disable** or **Enable** for **Proxy ARP**.

   Proxy ARP is an IP mechanism a Layer 3 switch can use to answer an ARP request on behalf of a host, by replying with the Layer 3 switch's own MAC address instead of the host.
10. Click **Disable** or **Enable** for **RARP**.

    Reverse ARP (RARP) is an IP mechanism a host can use to request an IP address from a directly attached Layer 3 switch when the host boots.
11. Click **Disable** or **Enable** for **Broadcast Forward**.
12. Click **Disable** or **Enable** for **Directed Broadcast Forward**.

    A directed broadcast is a packet containing all ones (or in some cases, all zeros) in the host portion of the destination IP address. When a Layer 3 switch forwards such a broadcast, it sends a copy of the packet to each of its enabled IP interfaces.
13. Click **Disable** or **Enable** for **Source Route**.
14. Click **Disable** or **Enable** for **Access Control List**.
15. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

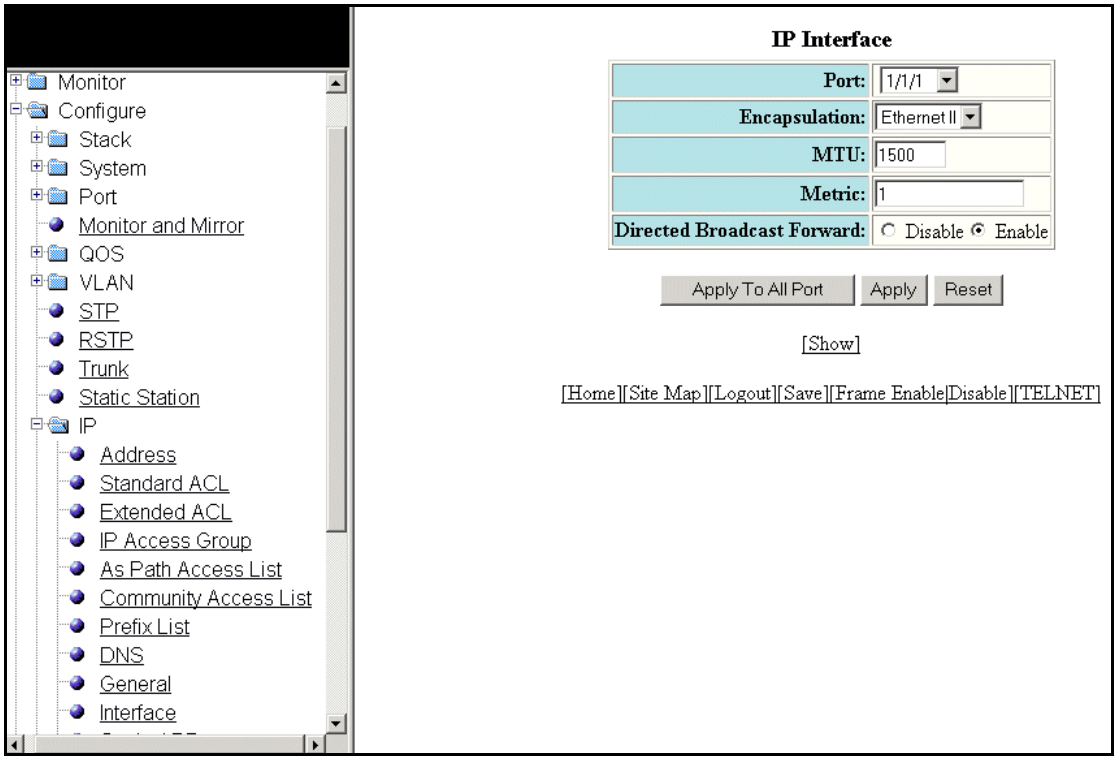
Configuring IP interfaces

To configure an IP interface, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Interface**.

The **IP Interface** window is displayed as shown in Figure 159.

FIGURE 159 Configuring an IP interface



3. Select a port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Select the format of the Layer 2 packets in the **Encapsulation** list.
5. Type the maximum size of the IP packet when encapsulated in a Layer 2 packet, in the **MTU** field.
6. Type the cost in the **Metric** field.
7. Click **Disable** or **Enable** for **Directed Broadcast Forward**.
8. Click **Apply** to configure the IP interface to the specified port or click **Apply To All Ports** to configure the IP interface on all the ports.

The message **The change has been made** is displayed. To display the configured IP interface, click **Show**. To reset the data entered in the configuration pane, click **Reset**.

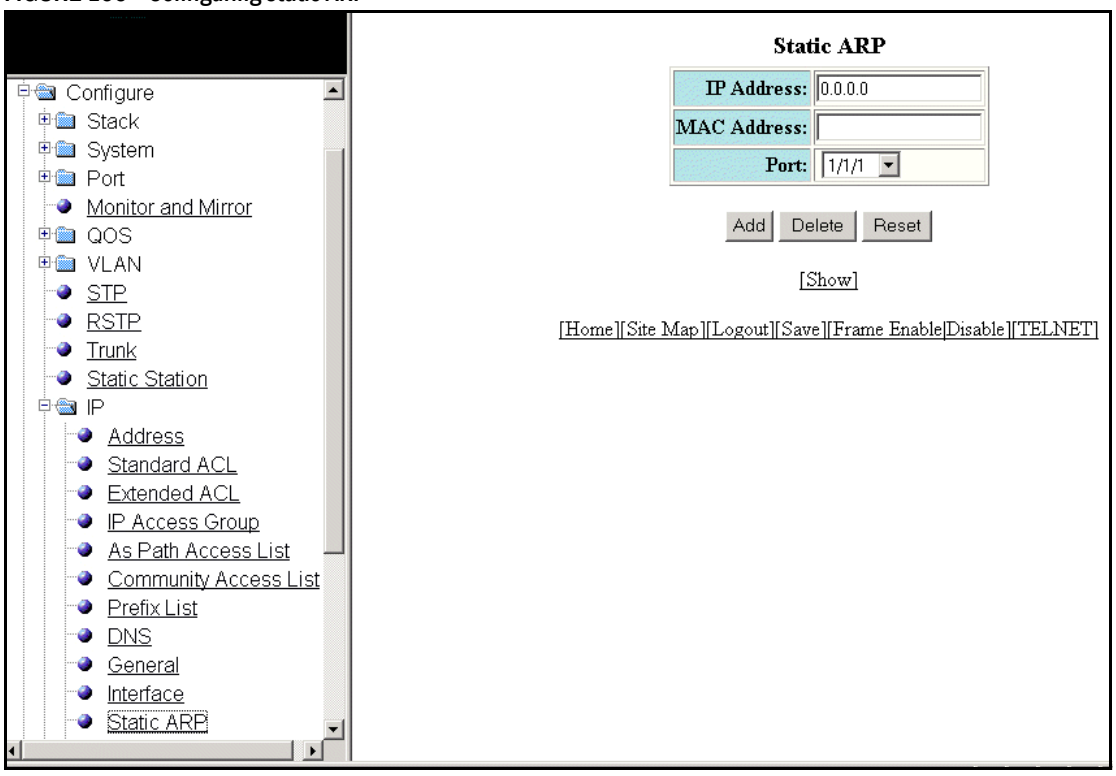
Configuring a static ARP

To configure a static Address Resolution Protocol (ARP) entry, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Static ARP**.

The **Static ARP** window is displayed as shown in Figure 160.

FIGURE 160 Configuring static ARP



3. Type the IP address of the directly connected device in the **IP Address** field.
4. Type the MAC address of the device in xx-xx-xx-xx-xx-xx format in the **MAC Address** field.
5. Select a port number in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured static ARP entry, click **Show**.

To delete the configured static ARP entry, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a static RARP

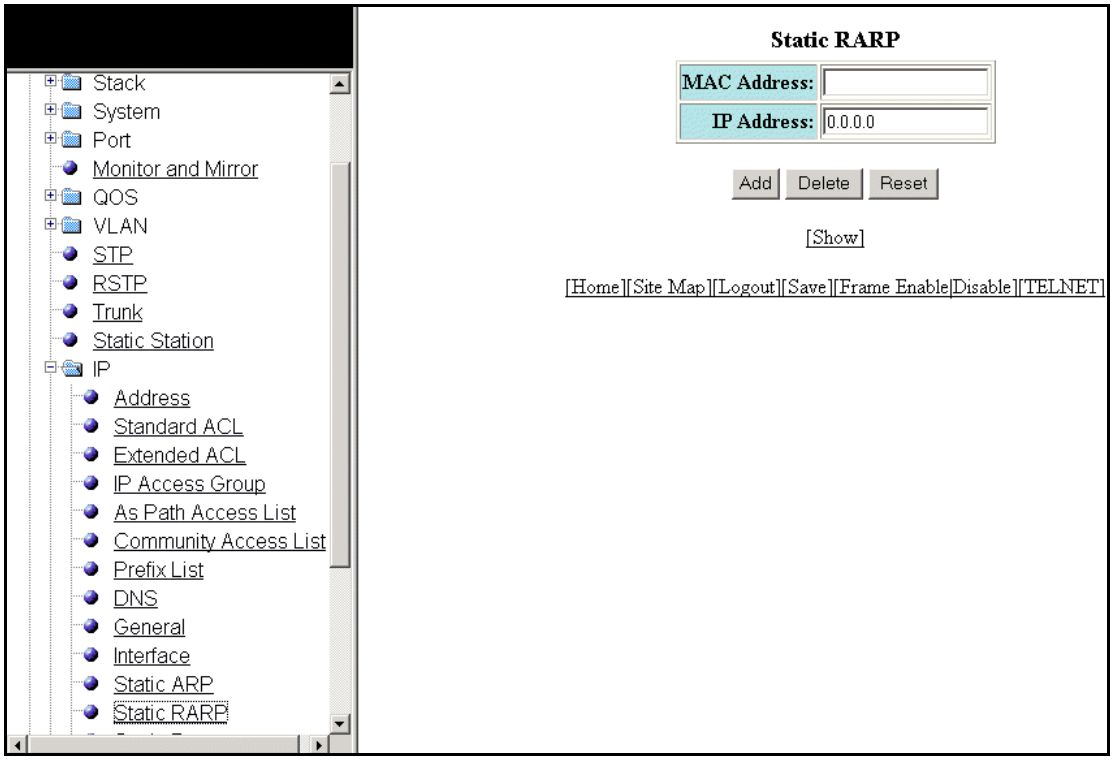
The Reverse Address Resolution Protocol (RARP) provides a simple mechanism for directly attached IP hosts to boot over the network. RARP allows an IP host that does not have a means of storing its IP address across power cycles or software reloads to query a directly attached Layer 3 switch for an IP address.

To configure a static IP RARP entry for static routes on a Brocade Layer 3 switch, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Static RARP**.

The **Static RARP** window is displayed as shown in Figure 161.

FIGURE 161 Configuring static RARP



3. Type the MAC address of the boot client in xx-xx-xx-xx-xx-xx format in the **MAC Address** field.
4. Type the IP address you want the Layer 3 switch to give to the client in the **IP Address** field.
5. Click **Add**.

The message **The change has been made** is displayed. To display the configured static IP RARP entry, click **Show**.

To delete the configured static IP RARP entry, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

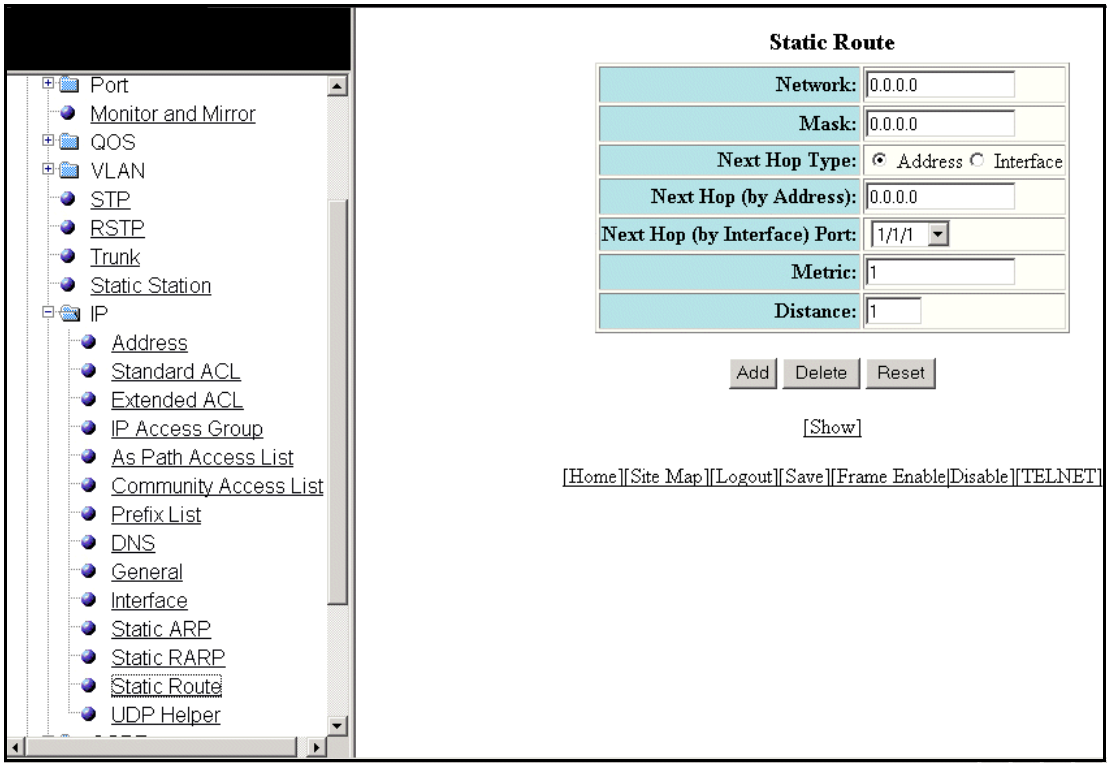
Configuring a static route

To configure an IP static route, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **Static Route**.

The **Static Route** window is displayed as shown in Figure 162.

FIGURE 162 Configuring static routes



3. Type the route destination IP address in the **Network** field.
4. Type the network mask in the **Mask** field.
5. Click **Address** for **Next Hop Type** and type the IP address of the next hop router (gateway) for the route in the **Next Hop (by Address)** field.

   Or

   Click **Interface** for **Next Hop Type** and select an Ethernet port in the **Next Hop (by Interface) Port** list.
6. Type the metric value from 1 through 16 in the **Metric** field. The default is one.
7. Type the administrative distance of the route in the **Distance** field. The default is one.
8. Click **Add**.

The message **The change has been made** is displayed. To display the configured static route, click **Show**.

To delete the configured static route, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

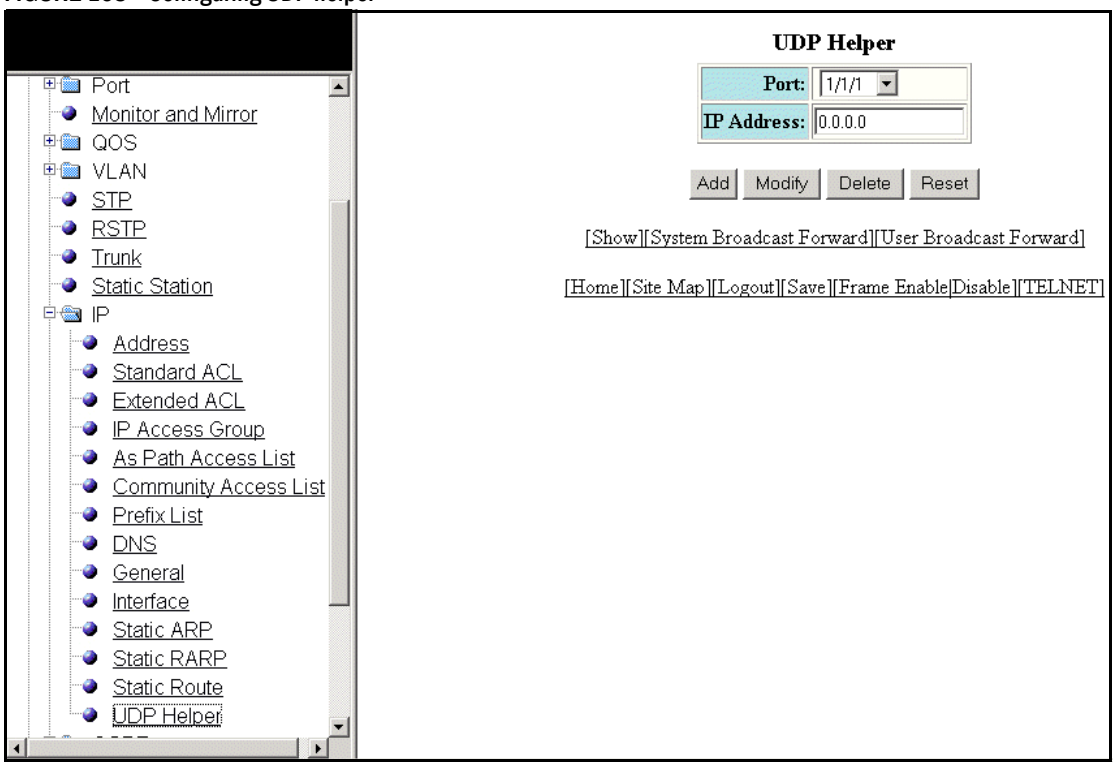
Configuring a UDP helper

To configure a helper address on the interface connected to the clients, perform the following steps.

1. Click **Configure** on the left pane and select **IP**.
2. Click **UDP Helper**.

The **UDP Helper** window is displayed as shown in Figure 163.

FIGURE 163 Configuring UDP helper



3. Select an Ethernet port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Type the server IP address or the subnet directed broadcast address of the IP subnet the server belongs to in the **IP Address** field.
5. Click **Add**.

The message **The change has been made** is displayed. To display the configured UDP helper, click **Show**.

To modify the configured UDP helper, click **Modify**. You can also delete the UDP helper by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

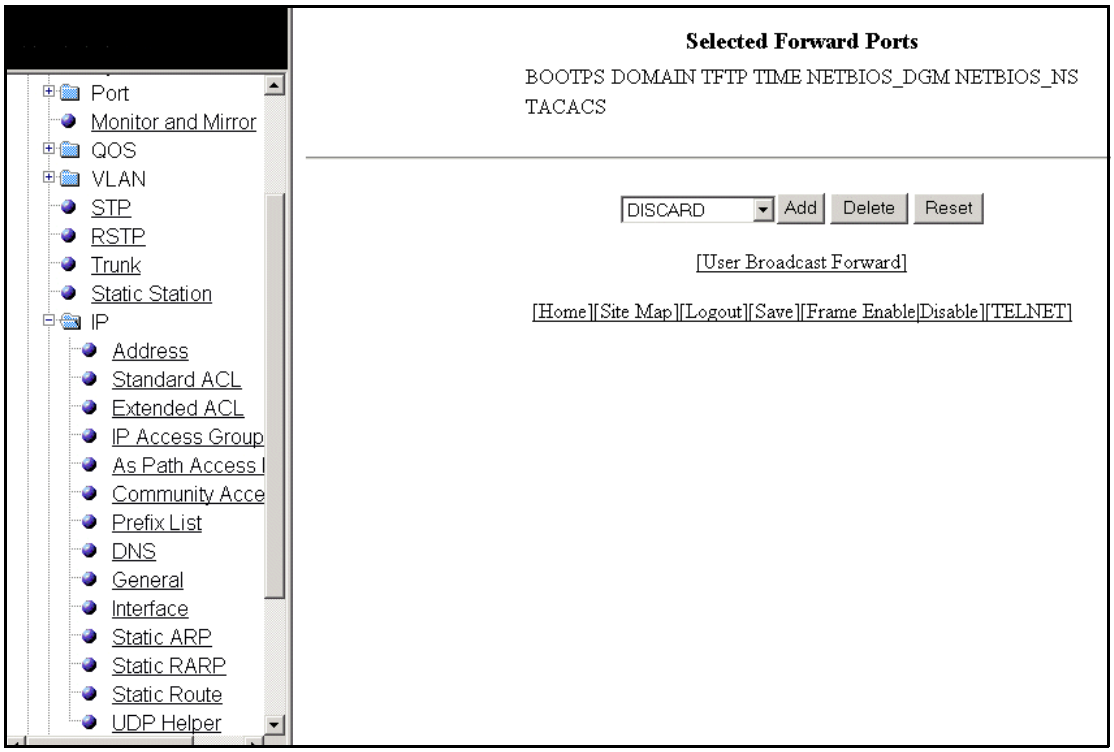
Enabling forwarding for a UDP application

To specify a UDP application by using an application name, perform the following steps.

1. Click **System Broadcast Forward** on the **UDP Helper** window.

The system broadcast forward window is displayed as in Figure 164.

FIGURE 164 Enabling forwarding for a UDP application



2. Select one of the following forward ports in the list:

- **BOOTPC**
- **BOOTPS**
- **DISCARD**
- **DNSIX**
- **DOMAIN**
- **ECHO**
- **MOBILE-IP**
- **NETBIOS-DGM**
- **NTP**
- **RIP**
- **SNMP**
- **SNMP-TRAP**
- **TACACS**
- **TALK**

- TFTP
- TIME

3. Click **Add**.

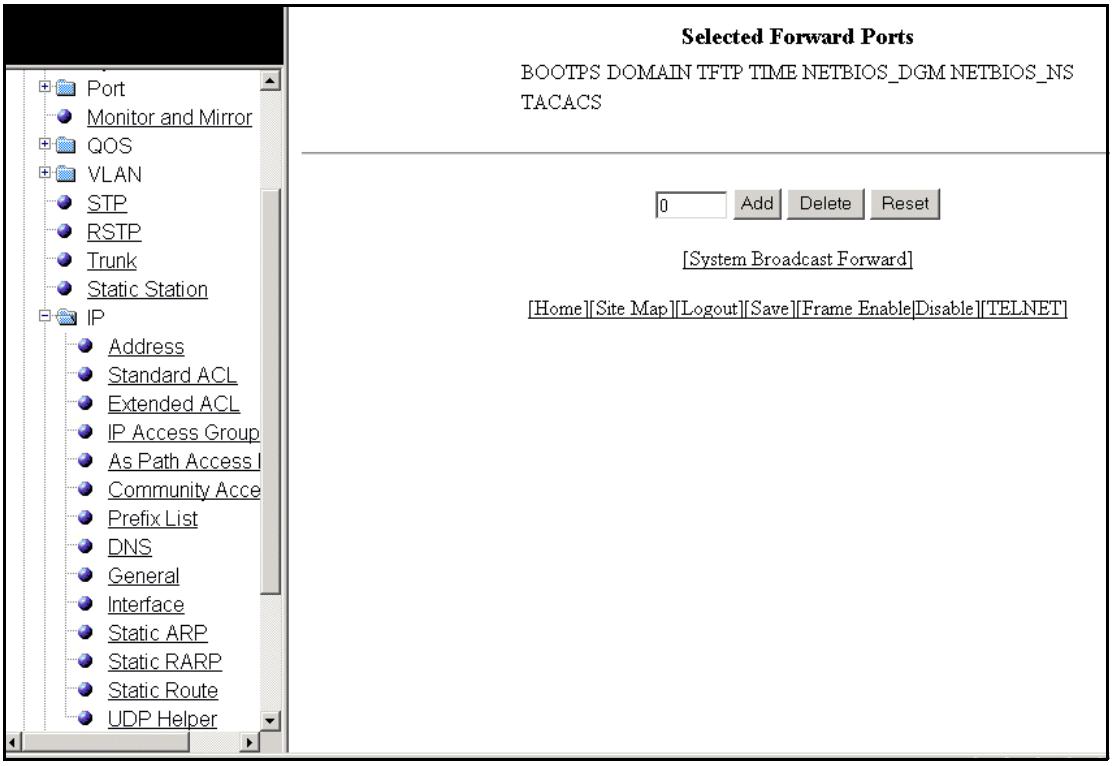
The added port is displayed in the **Selected Forward Ports** pane, which displays the application ports that are enabled by default. To delete the forwarding port, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

To specify a UDP application by using an application UDP port number, perform the following steps.

1. Click **User Broadcast Forward** on the **UDP Helper** window.

The user broadcast forward window is displayed as shown in Figure 165.

FIGURE 165 Enabling user broadcast forward



2. Type the UDP port number in the field.
3. Click **Add**.

The added port is displayed in the **Selected Forward Ports** pane, which displays the application ports that are enabled by default.

To delete the forwarding port, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

26

Configuring OSPF

In this chapter

- Configuring an OSPF area 239
- Configuring the OSPF area range 240
- Configuring the general OSPF settings 242
- Configuring OSPF interfaces 243
- Configuring an OSPF redistribution filter 245
- Configuring OSPF virtual link interfaces 247
- Configuring an OSPF trap 248

NOTE
The Open Shortest Path First (OSPF) feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

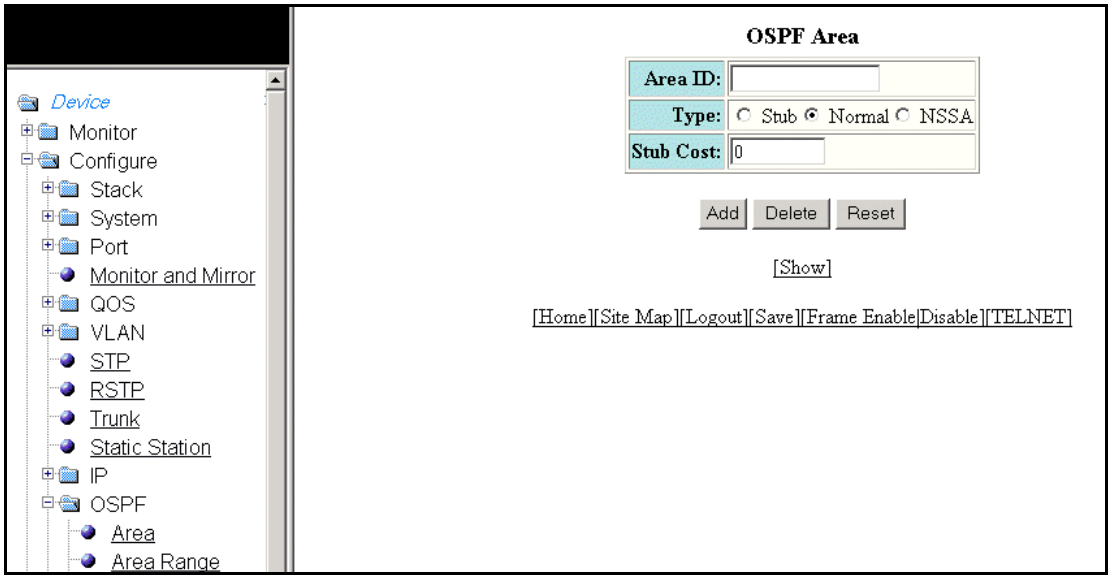
Configuring an OSPF area

To configure an OSPF area, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **Area**.

The **OSPF Area** window is displayed as shown in Figure 166.

FIGURE 166 Configuring an OSPF area



3. Type an IP address or number as the area identifier in the **Area ID** field. If you specify a number, it should be from 0 through 18.
4. Click one of the following options for **Type**:
   - **Stub** - OSPF Layer 3 switches within a stub area cannot send or receive External Link State Advertisements (LSAs). In addition, OSPF Layer 3 switches in a stub area use a default route to the Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) to send traffic out of the area.
   - **Normal** - OSPF Layer 3 switches within a normal area can send and receive External LSAs.
   - **NSSA** - The ASBR of a Not-So-Stubby Area (NSSA) can import external route information into the area.
5. Type an area cost from 1 through 16777215 in the **Stub Cost** field.
6. Click **Add**.

The message **The change has been made is displayed** and the OSPF area is configured. To display the configured OSPF area, click **Show**.

To reset the data entered in the configuration pane, click **Reset**. You can also delete the OSPF area by clicking **Delete**.

Configuring the OSPF area range

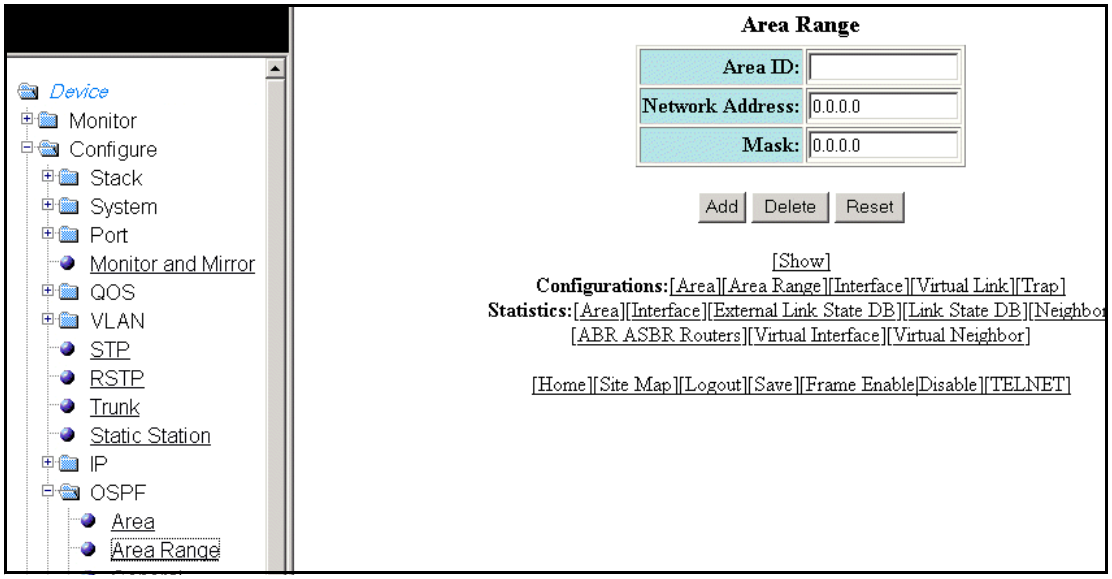
Area range allows a specific IP address and mask to represent a range of IP addresses within an area, so that only that reference range address is advertised to the network instead of all the addresses within that range. Each area can have up to 32 addresses.

To configure an OSPF area range, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **Area Range**.

The **Area Range** window is displayed as shown in Figure 167.

FIGURE 167 Configuring the area range



3. Type an area identifier in the **Area ID** field.
4. Type a network IP address in the **Network Address** field.
5. Type an IP subnet mask address in the **Mask** field.
6. Click **Add**.

The message **The change has been made** is displayed and the OSPF area range is configured. To display the configured OSPF area range, click **Show**.

To reset the data entered in the configuration pane, click **Reset**. You can also delete the OSPF area range by clicking **Delete**.

The **Area Range** window provides links to configure and monitor OSPF parameters.

- The **Configurations** links can be used for configuring the OSPF parameters:
  - To configure OSPF area, click **Area**. For more information, refer to "Configuring an OSPF area" on page 239.
  - To configure OSPF area range, click **Area Range**. For more information, refer to "Configuring the OSPF area range" on page 240.
  - To configure OSPF interfaces, click **Interface**. For more information, refer to "Configuring OSPF interfaces" on page 243.
  - To configure OSPF virtual links, click **Virtual Link**. For more information, refer to "Configuring OSPF virtual link interfaces" on page 247.
  - To configure OSPF traps, click **Trap**. For more information, refer to "Configuring an OSPF trap" on page 248.
- The **Statistics** links can be used to monitor the OSPF parameters:
  - To display OSPF area information, click **Area**. For more information, refer to "Displaying OSPF area information" on page 71.
  - To display the OSPF interface information, click **Interface**. For more information, refer to "Displaying the OSPF interfaces" on page 75.
  - To display the OSPF external link-state database information, click **External Link State DB**. For more information, refer to "Displaying OSPF external link-state database" on page 73.
  - To display the link-state database information, click **Link State DB**. For more information, refer to "Displaying OSPF link state database" on page 78.
  - To display the OSPF neighbor information, click **Neighbor**. For more information, refer to "Displaying OSPF neighbors" on page 80.
  - To display the OSPF ABR ASBR router information, click **ABR ASBR Routers.** For more information, refer to "Displaying the OSPF ABR ASBR router information" on page 69.
  - To display the OSPF virtual interfaces information, click **Virtual Interface**. For more information, refer to "Displaying OSPF virtual interfaces" on page 82.
  - To display the OSPF virtual neighbor information, click **Virtual Neighbor**. For more information, refer to "Displaying OSPF virtual neighbors" on page 85.

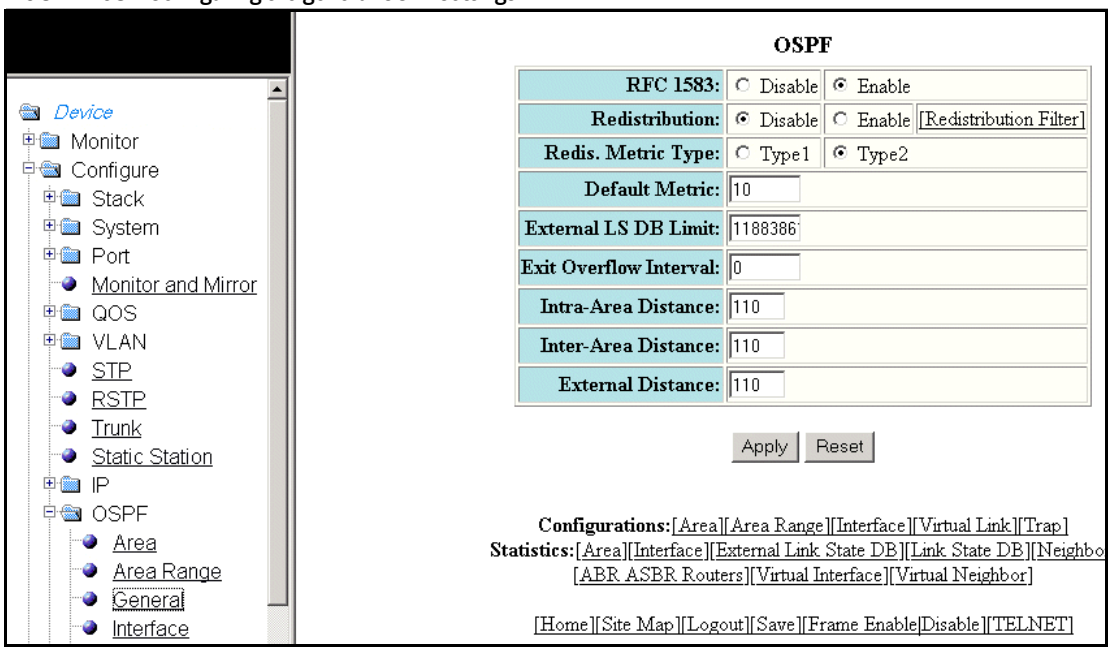
Configuring the general OSPF settings

To configure the general settings for OSPF, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **General**.

The **OSPF** window is displayed as shown in Figure 168.

FIGURE 168 Configuring the general OSPF settings



3. Click **Disable** or **Enable** for **RFC 1583**. By default, Brocade Layer 3 switches are configured to be compliant with the RFC 1583 OSPF specification. If you click **Disable**, the Layer 3 switch operates with the latest OSPF standard, RFC 2178.
4. Click **Disable** or **Enable** for **Redistribution**. To configure an OSPF redistribution filter, click **Redistribution Filter**. For more information on how to configure a redistribution filter, refer to "Configuring an OSPF redistribution filter" on page 245.
5. Click **Type 1** or **Type 2** for **Redis.Metric Type**. By default, **Type 2** is enabled.
6. Type the default metric in the **Default Metric** field.

   The default metric is a global parameter that specifies the cost applied to all the OSPF routes. You can assign a cost from 1 through 15. The default value is 10.
7. Type the maximum number of external LSAs the link-state database can hold in the **External LS DB Limit** field.
8. Type the exit overflow interval in the **Exit Overflow Interval** field. The range is from 0 through 86400 seconds (24 hours). The default value is zero.

If a database overflow condition occurs on a Layer 3 switch, the Layer 3 switch eliminates the condition by removing entries that originated on the Layer 3 switch. The exit overflow interval allows you to set how often a Layer 3 switch checks to see if the overflow condition has been eliminated. If the configured value of the database overflow interval is zero, then the Layer 3 switch never leaves the database overflow condition.

9. Type the administrative distance for the intra-area Layer 3 switch in the **Intra-Area Distance** field. The default value is 110.
10. Type the administrative distance for the inter-area Layer 3 switch in the **Inter-Area Distance** field. The default value is 110.
11. Type the administrative distance for the external Layer 3 switch in the **External Distance** field. The default value is 110.
12. Click **Apply**.

The message **The change has been made** is displayed and the general settings for OSPF are configured. To reset the data entered in the configuration pane, click **Reset**.

The **OSPF** window provides links to configure and monitor OSPF parameters. For more information on the links, refer to the "Configuring the OSPF area range" on page 240.

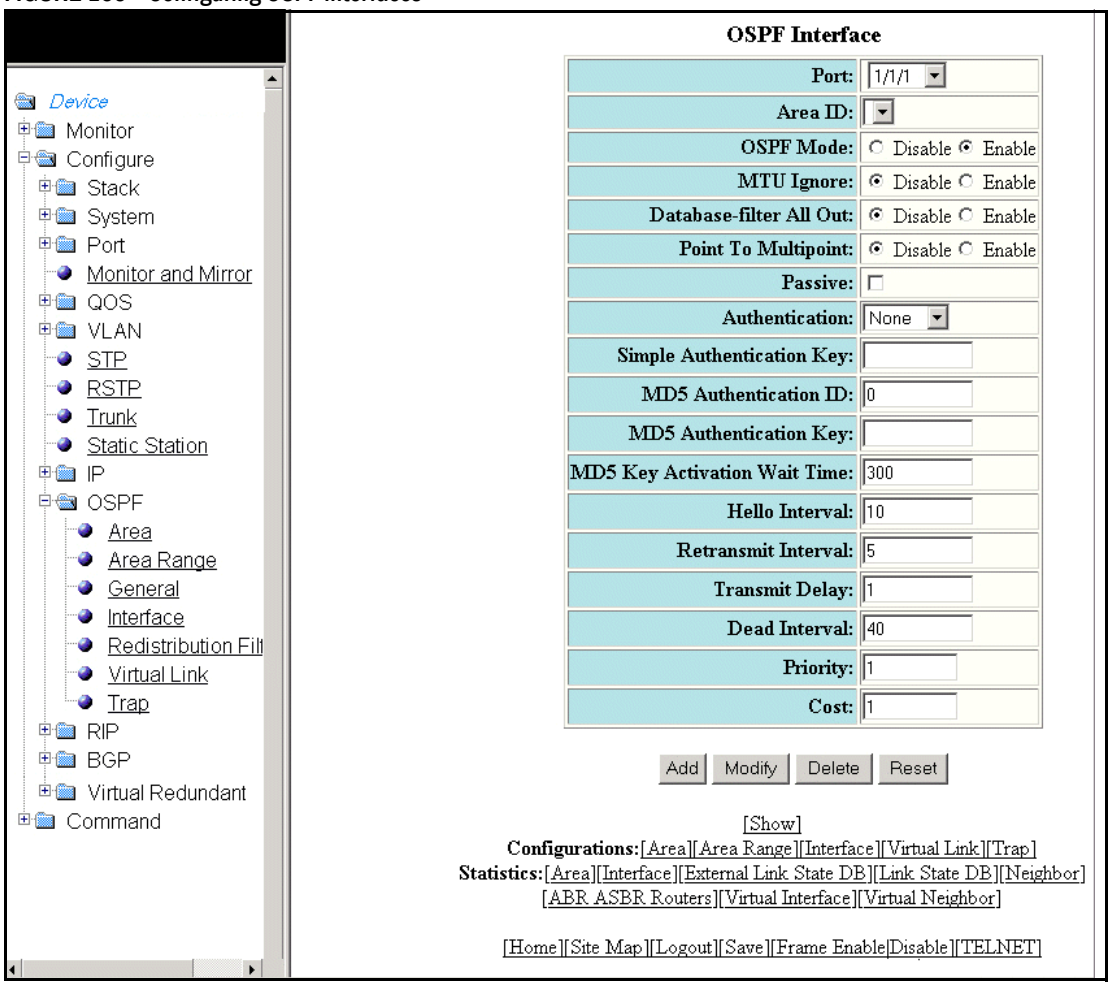
Configuring OSPF interfaces

To configure an OSPF interface, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **Interface**.

The **OSPF Interface** window is displayed as shown in Figure 169.

FIGURE 169 Configuring OSPF interfaces



3. Select a port number in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
4. Select an OSPF area identifier in the **Area ID** list.
5. Click **Disable** or **Enable** for **OSPF Mode**.
6. Click **Disable** or **Enable** for **MTU Ignore**.
7. Click **Disable** or **Enable** for **Database-filter All Out**. By clicking **Enable**, you can configure a filter to block outbound LSAs on an OSPF interface.
8. Click **Disable** or **Enable** for **Point to Multipoint**.
9. Select the **Passive** check box to restrict the interface to send or receive OSPF route updates.
10. Select one of the following authentication types in the **Authentication** list:
    - **None**
    - **Simple**
    - **MD5**

11. Type an alphanumeric password for an interface in the **Simple Authentication Key** field.
12. Type the MD5 key identifier from 1 through 255 in the **MD5 Authentication ID** field.
13. Type the MD5 key, which can be up to 16 alphanumeric characters, in the **MD5 Authentication Key** field.
14. Type the MD5 authentication activation wait time in the **MD5 Key Activation Wait Time** field.

    The MD5 authentication activation wait time is the number of seconds the Layer 3 switch waits until placing a new MD5 key into effect. The wait time can be from 0 through 14400 seconds. The default is 300 seconds (5 minutes).
15. Type the number of seconds between the transmission of hello packets in the **Hello Interval** field. The value can be from 1 through 65535 seconds. The default is 10 seconds.
16. Type the time interval between retransmissions of link-state advertisements (LSAs) to adjacent Layer 3 switches for this interface in the **Retransmit Interval** field. The value can be from 0 through 3600 seconds. The default is five seconds.
17. Type the number of seconds it takes to transmit link-state update packets on this interface in the **Transit Delay** field. The value can be from 0 through 3600 seconds. The default is one second.
18. Type the number of seconds that a neighbor Layer 3 switch waits for a hello packet from the current Layer 3 switch before declaring the Layer 3 switch down in the **Dead Interval** field. The value can be from 1 through 65535 seconds. The default is 40 seconds.
19. Type the priority for selecting the Designated Router (DR) and Backup Designated Routers (BDRs) in the **Priority** field. If you set the priority to 0, the Layer 3 switch does not participate in the DR and BDR election.
20. Type the cost required to send a packet across an interface in the **Cost** field.
21. Click **Add**.

The message **The change has been made** is displayed. To change the configured values, click **Modify**. You can also delete the configured OSPF interface by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **OSPF Interface** window provides links to configure and monitor OSPF parameters. For more information on the links, refer to the "Configuring the OSPF area range" on page 240.

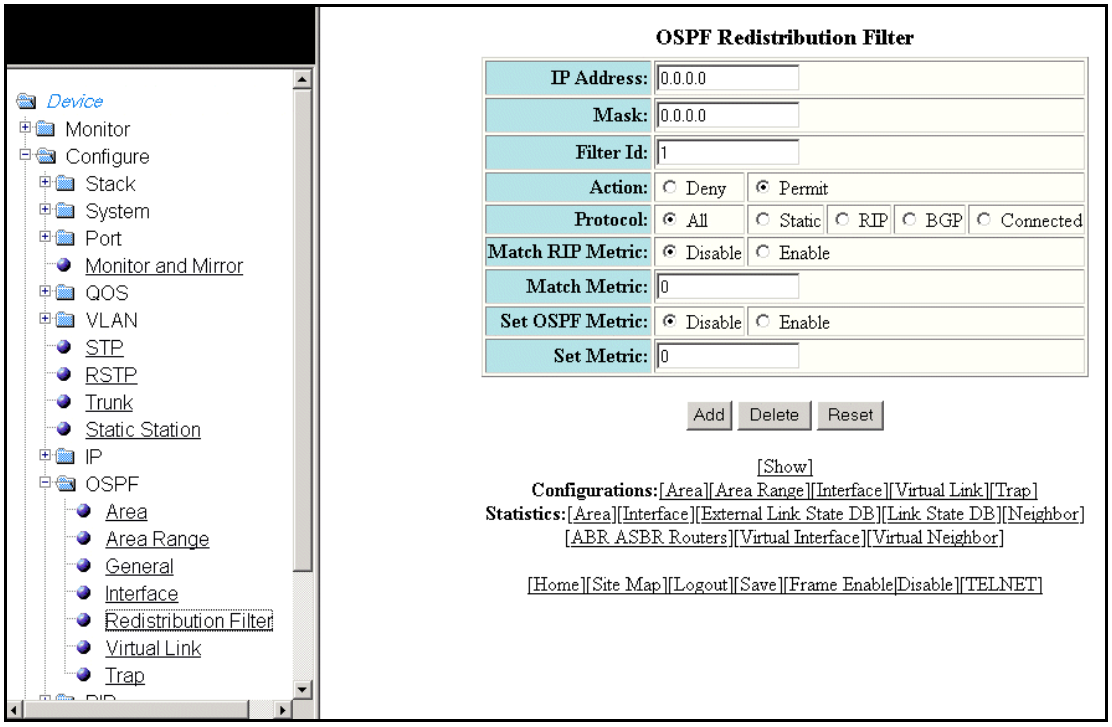
Configuring an OSPF redistribution filter

To configure an OSPF redistribution filter, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **Redistribution Filter**.

The **OSPF Redistribution Filter** window is displayed as shown in Figure 170.

FIGURE 170 Configuring the OSPF redistribution filter



3. Type the IP address of the device in the **IP Address** field.
4. Type the IP subnet mask address in the **Mask** field.
5. Type a redistribution filter identifier in the **Filter Id** field.
6. Click **Deny** or **Permit** for **Action**.
7. Click one of the following options for **Protocol**:
   - **All** - Applies redistribution to all route types.
   - **Static** - Applies redistribution to IP static routes only.
   - **RIP** - Applies redistribution to RIP routes only.
   - **BGP** - Applies redistribution to BGP routes only.
   - **Connected** - Applies redistribution to a directly connected network.
8. Click **Disable** or **Enable** for **Match RIP Metric**.
9. Type a match metric value in the **Match Metric** field. The match metric parameter applies the redistribution filter only to those routes with the specified metric value.
10. Click **Disable** or **Enable** for **Set OSPF Metric**.
11. Type the OSPF metric value that will be applied to those routes imported into OSPF in the **Set Metric** field.
12. Click **Add**.

The message **The change has been made** is displayed and the OSPF redistribution filter is configured. To display the configured OSPF redistribution filter, click **Show**.

To delete the configured OSPF redistribution filter, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **OSPF Redistribution Filter** window provides links to configure and monitor OSPF parameters. For more information on the links, refer to the "Configuring the OSPF area range" on page 240.

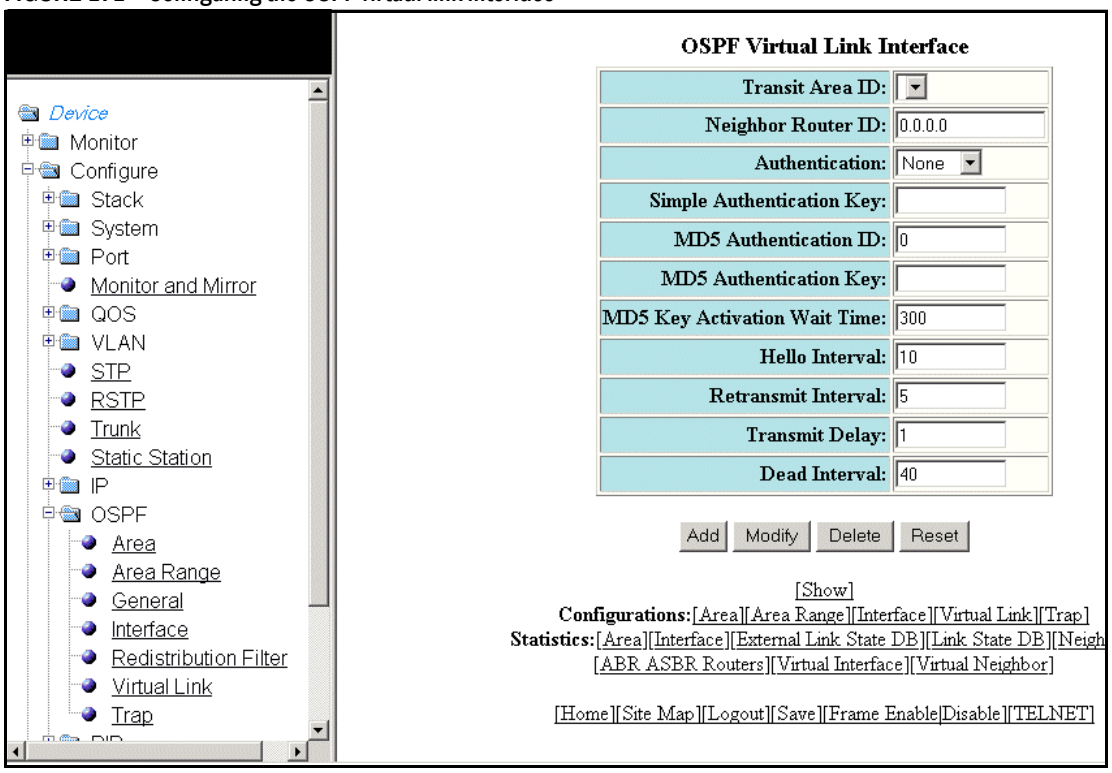
Configuring OSPF virtual link interfaces

To configure an OSPF virtual link interface, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **Virtual Link**.

The **OSPF Virtual Link Interface** window is displayed as shown in Figure 171.

FIGURE 171 Configuring the OSPF virtual link interface



3. Select a transit area identifier in the **Transit Area ID** list.

   The transit area ID represents the shared area of the two ABRs and serves as the connection point between the two Layer 3 switches. This number should match the area ID value.

4. Type the IP address of the Layer 3 switch that is physically connected to the backbone in the **Neighbor Router ID** field.
5. Select one of the following authentication types in the **Authentication** list:
   - **None**
   - **Simple**
   - **MD5**

6. Type an alphanumeric password for an interface in the **Simple Authentication Key** field.
7. Type the MD5 key identifier from 1 through 255 in the **MD5 Authentication ID** field.
8. Type the MD5 key, which can be up to 16 alphanumeric characters, in the **MD5 Authentication Key** field.
9. Type the MD5 authentication activation wait time in the **MD5 Key Activation Wait Time** field.

   The MD5 authentication activation wait time is the number of seconds the Layer 3 switch waits until placing a new MD5 key into effect. The wait time can be from 0 through 14400 seconds. The default is 300 seconds (5 minutes).
10. Type the hello interval in the **Hello Interval** field. The value can be from 1 through 65535 seconds. The default is 10 seconds.
11. Type the retransmission interval in the **Retransmit Interval** field. The value can be from 0 through 3600 seconds. The default is five seconds.
12. Type the transmission delay in the **Transit Delay** field. The value can be from 0 through 3600 seconds. The default is one second.
13. Type the dead interval in the **Dead Interval** field. The value can be from 1 through 65535 seconds. The default is 40 seconds.
14. Click **Add**.

The message **The change has been made** is displayed. To change the configured values, click **Modify**. You can also delete the configured OSPF virtual link interface by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **OSPF Virtual Link Interface** window provides links to configure and monitor OSPF parameters. For more information on the links, refer to the "Configuring the OSPF area range" on page 240.

Configuring an OSPF trap

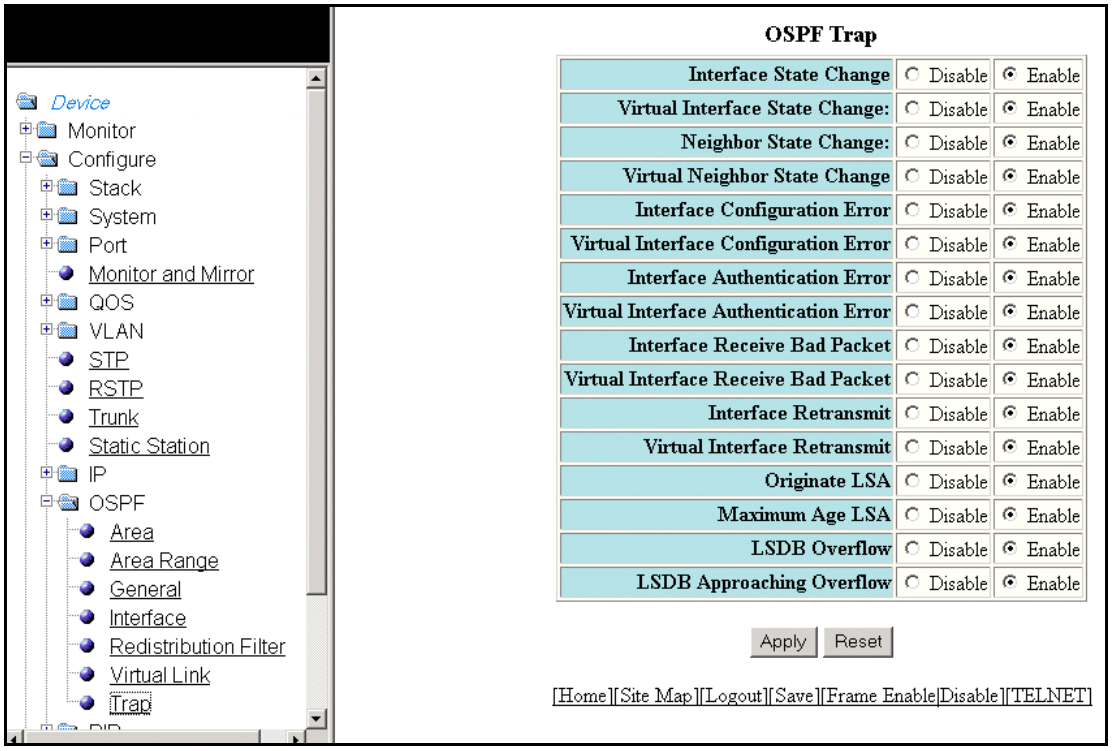
OSPF traps as defined by RFC 1850 are supported on Brocade Layer 3 switches. By default, OSPF trap generation is enabled on the Layer 3 switch.

To disable all or a specific OSPF trap generation, perform the following steps.

1. Click **Configure** on the left pane and select **OSPF**.
2. Click **Trap**.

The **OSPF Trap** window is displayed as shown in Figure 172.

FIGURE 172 Configuring the OSPF trap



3. Select **Disable** or **Enable** for **Interface State Change**.
4. Select **Disable** or **Enable** for **Virtual Interface State Change**.
5. Select **Disable** or **Enable** for **Neighbor State Change**.
6. Select **Disable** or **Enable** for **Virtual Neighbor State Change**.
7. Select **Disable** or **Enable** for **Interface Configuration Error**.
8. Select **Disable** or **Enable** for **Virtual Interface Configuration Error**.
9. Select **Disable** or **Enable** for **Interface Authentication Error**.
10. Select **Disable** or **Enable** for **Virtual Interface Authentication Error**.
11. Select **Disable** or **Enable** for **Interface Receive Bad Packet**.
12. Select **Disable** or **Enable** for **Virtual Interface Receive Bad Packet**.
13. Select **Disable** or **Enable** for **Interface Retransmit**.
14. Select **Disable** or **Enable** for **Virtual Interface Retransmit**.
15. Select **Disable** or **Enable** for **Originate LSA**.
16. Select **Disable** or **Enable** for **Maximum Age LSA**.
17. Select **Disable** or **Enable** for **LSDB Overflow**.
18. Select **Disable** or **Enable** for **LSDB Approaching Overflow**.
19. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

Chapter

27

Configuring RIP

In this chapter

- Configuring the general RIP settings 251
- Configuring a RIP interface 252
- Configuring a RIP neighbor filter 255
- Configuring a RIP route filter 256
- Configuring a RIP redistribution filter 258

NOTE
The Routing Information Protocol (RIP) feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

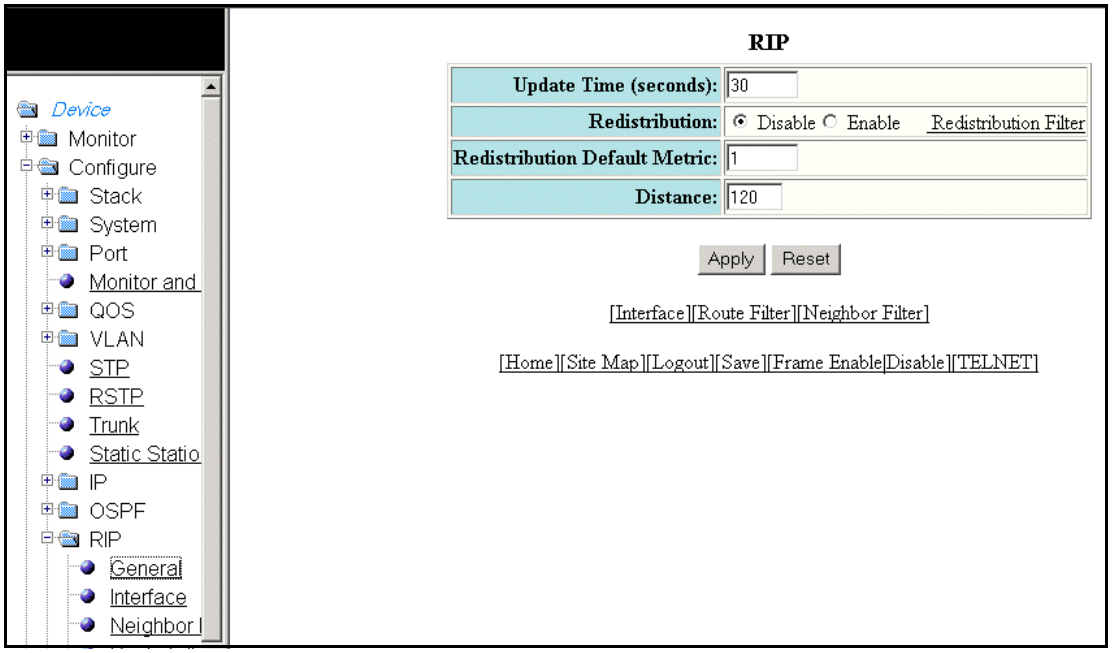
Configuring the general RIP settings

To configure the general RIP settings, perform the following steps.

1. Click **Configure** on the left pane and select **RIP**.
2. Click **General**.

The **RIP** window is displayed as shown in Figure 173.

FIGURE 173 Configuring the general RIP settings



3. Type the update interval from 1 through 1000 seconds in the **Update Time (seconds)** field. The default value is 30 seconds.

   The update interval specifies how often the Layer 3 switch sends route advertisements to its RIP neighbors.

4. Click **Disable** or **Enable** for **Redistribution**. To configure a redistribution filter, click **Redistribution Filter**. For more information on how to configure a RIP redistribution filter, refer to "Configuring a RIP redistribution filter" on page 258.

5. Type the RIP cost from 1 through 15 in the **Redistribution Default Metric** field. The default is one.

6. Type the administrative distance of the RIP Layer 3 switches in the **Distance** field. The default value is 120.

7. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

The **RIP** window provides links to configure other RIP parameters:

- To configure a RIP interface, click **Interface**. For more information, refer to "Configuring a RIP interface" on page 252.
- To configure a RIP route filter, click **Route Filter**. For more information, refer to "Configuring a RIP route filter" on page 256.
- To configure a RIP neighbor filter, click **Neighbor Filter**. For more information, refer to "Configuring a RIP neighbor filter" on page 255.

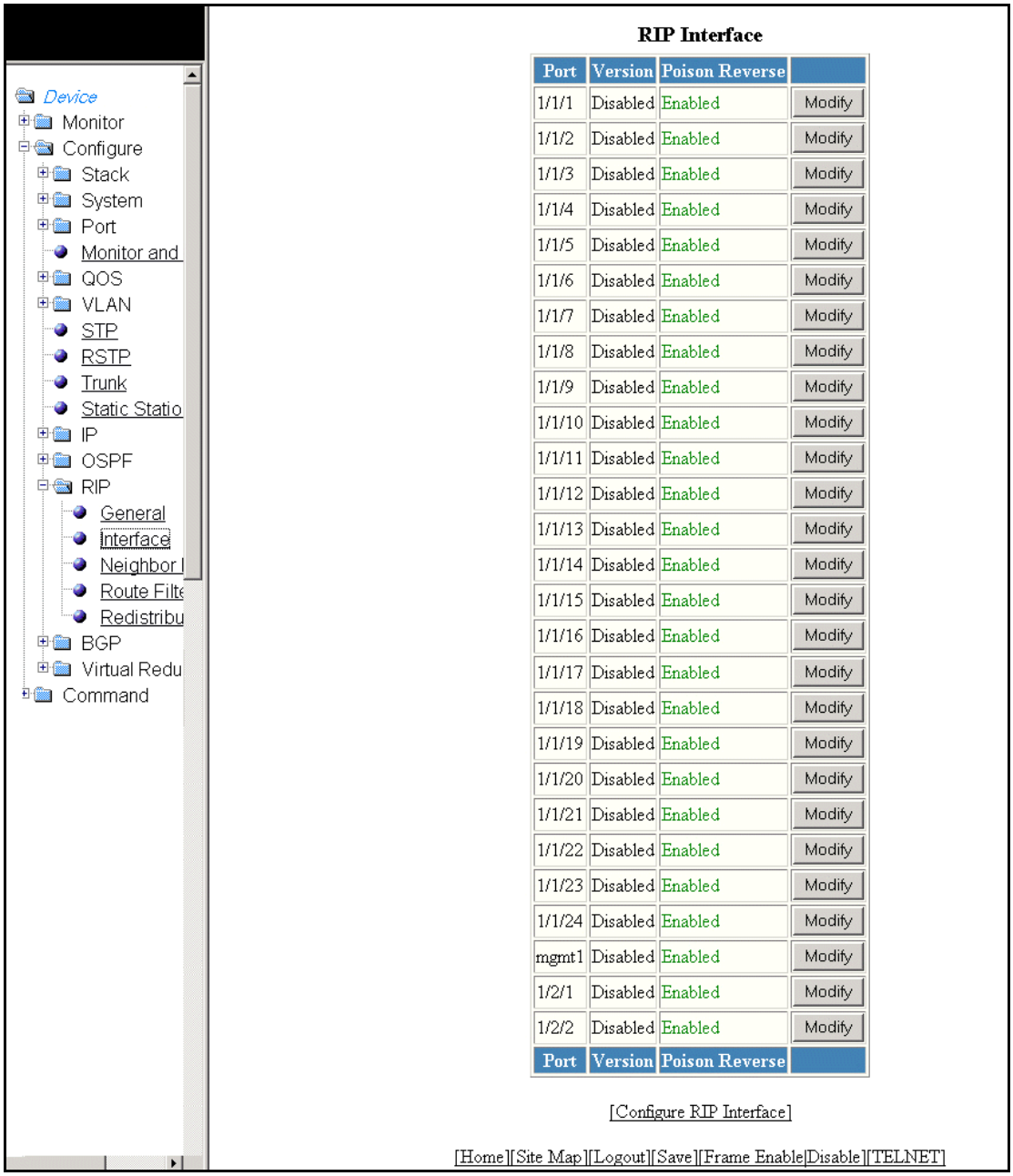
Configuring a RIP interface

To configure a RIP interface, perform the following steps.

1. Click **Configure** on the left pane and select **RIP**.
2. Click **Interface**.

The **RIP Interface** window is displayed as shown in Figure 174.

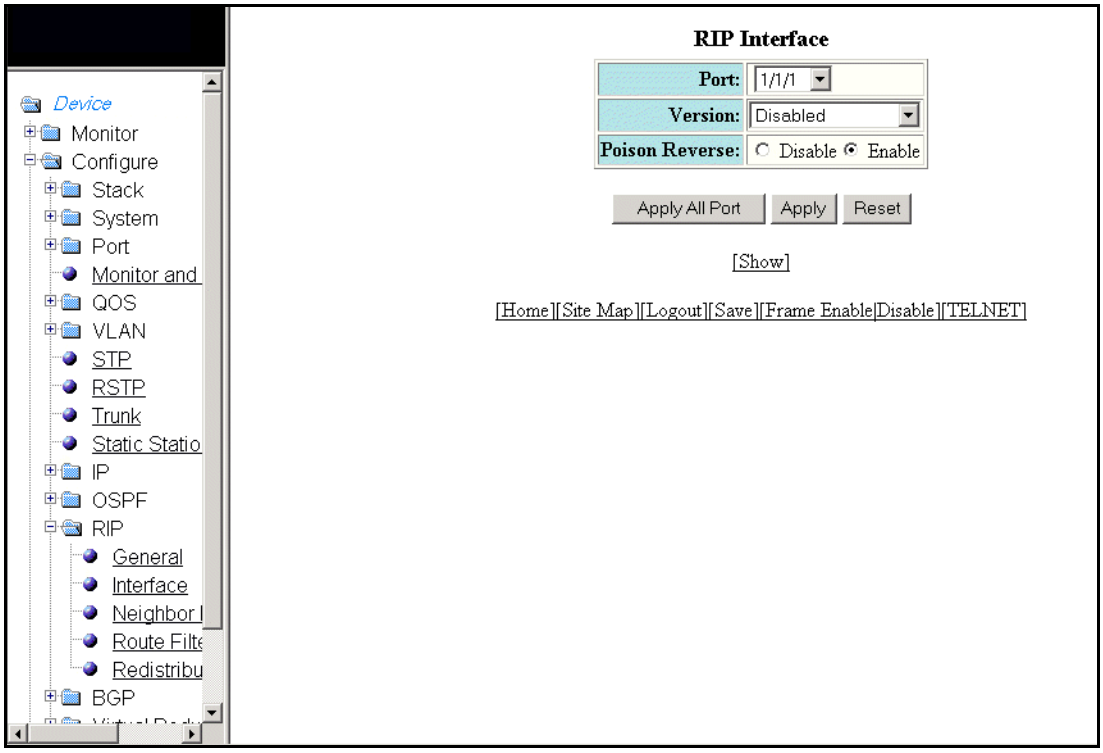
FIGURE 174 RIP interface



3. Click **Configure RIP Interface** or **Modify** to change the RIP interface parameters for the respective port.

The **RIP Interface** window is displayed as shown in Figure 175.

FIGURE 175 Configuring a RIP interface



4. Select a port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
5. Select one of the following options for **Version**:
   - **Disabled**
   - **V1 Only**
   - **V2 Only**
   - **V1-Compatible-V2**
6. Click **Disable** or **Enable** for **Poison Reverse**.

   Poison reverse is the method a Layer 3 switch uses to prevent routing loops caused by advertising a route on the same interface as the one on which the Layer 3 switch learned the route.
7. Click **Apply** to configure the RIP interface to the specified port or click **Apply All Port** to configure the RIP interface on all the ports.

The message **The change has been made** is displayed. To display the configured RIP interface, click **Show**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a RIP neighbor filter

By default, a Brocade Layer 3 switch learns RIP routes from all its RIP neighbors. Neighbor filters allow you to specify the neighbor Layer 3 switches from which the Brocade device can receive RIP routes. Neighbor filters apply globally to all ports.

To configure a RIP neighbor filter, perform the following steps.

1. Click **Configure** on the left pane and select **RIP**.
2. Click **Neighbor Filter**.

The **RIP Neighbor Filter** window is displayed as shown in Figure 176.

FIGURE 176 Configuring a RIP neighbor filter

3. Type a filter number in the **ID** field.
4. Click **Deny** or **Permit** for **Action**.
5. Type a source IP address in the **Source IP** field.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured RIP neighbor filter, click **Show**.

To modify the configured RIP neighbor filter, click **Modify**. To reset the data entered in the configuration pane, click **Reset**. You can also delete the configured RIP neighbor filter by clicking **Delete**.

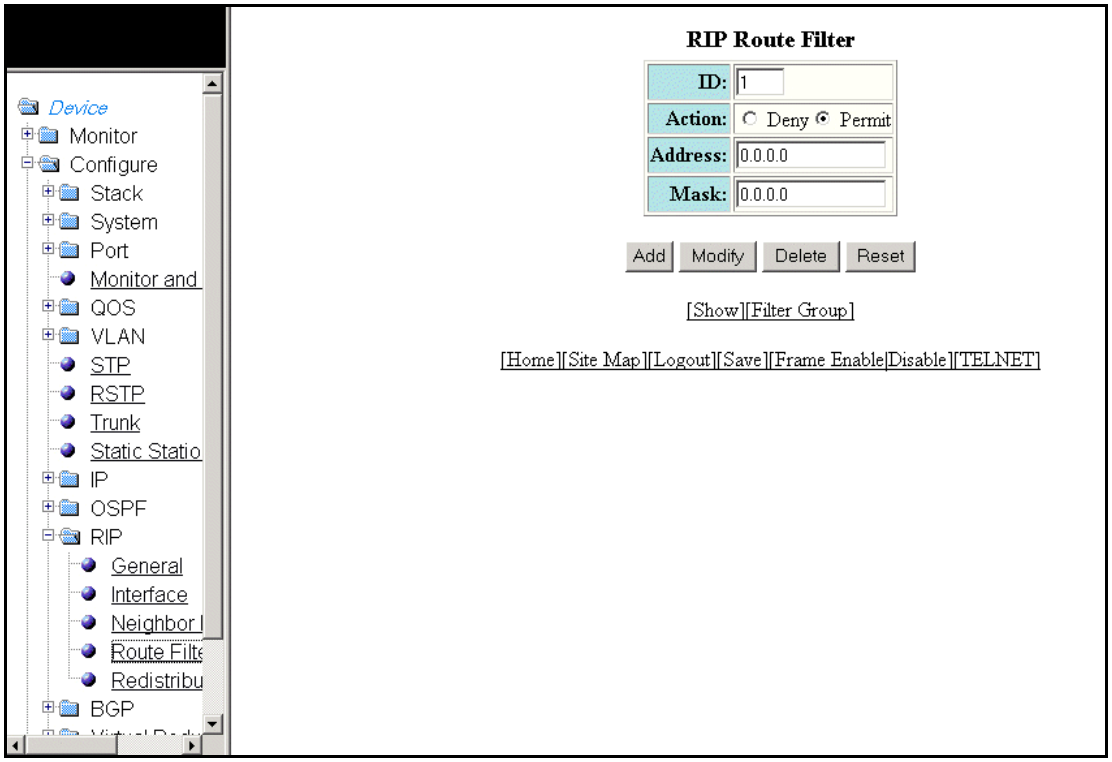
Configuring a RIP route filter

To configure a RIP route filter to permit or deny learning or advertising of specific routes, perform the following steps.

1. Click **Configure** on the left pane and select **RIP**.
2. Click **Route Filter**.

The **RIP Route Filter** window is displayed as shown in Figure 177.

FIGURE 177 Configuring a RIP route filter



3. Type a filter number in the **ID** field.
4. Click **Deny** or **Permit** for **Action**.
5. Type a source IP address in the **Address** field.
6. Type a source mask in the **Mask** field.
7. Click **Add**.

The message **The change has been made** is displayed. To display the configured RIP route filter, click **Show**.

To modify the configured RIP route filter, click **Modify**. To reset the data entered in the configuration pane, click **Reset**. You can also delete the configured RIP route filter by clicking **Delete**.

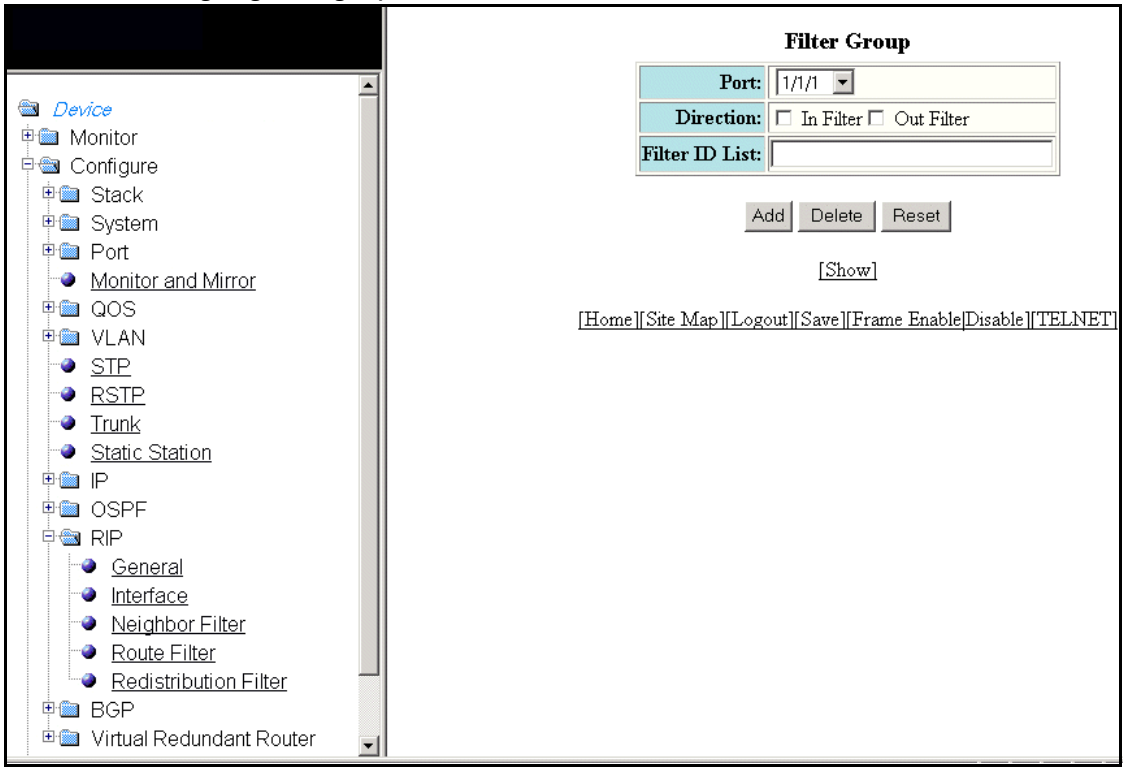
Configuring a filter group

After you define RIP route filters, you must assign them to individual interfaces. The filters do not take effect until you apply them to the interfaces. To apply RIP a route filter to an interface, perform the following steps.

1. Click **Filter Group** on the **RIP Route Filter** window.

The **Filter Group** window is displayed as shown in Figure 178.

FIGURE 178 Configuring a filter group



2. Select an Ethernet port in the **Port** list. The port number varies based on the product:
   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum
3. Select one of the following for **Directions**:
   - **In filters** - Applies to routes the Layer 3 switch learns from its neighbor on the interface.
   - **Out filters** - Applies to routes the Layer 3 switch advertises to its neighbor on the interface.
4. Type the RIP route filters that you want to apply for an interface in the **Filter ID List** field.
5. Click **Add**.

The message **The change has been made** is displayed. To display the configured RIP route filter group, click **Show**.

To delete the configured RIP route filter group, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

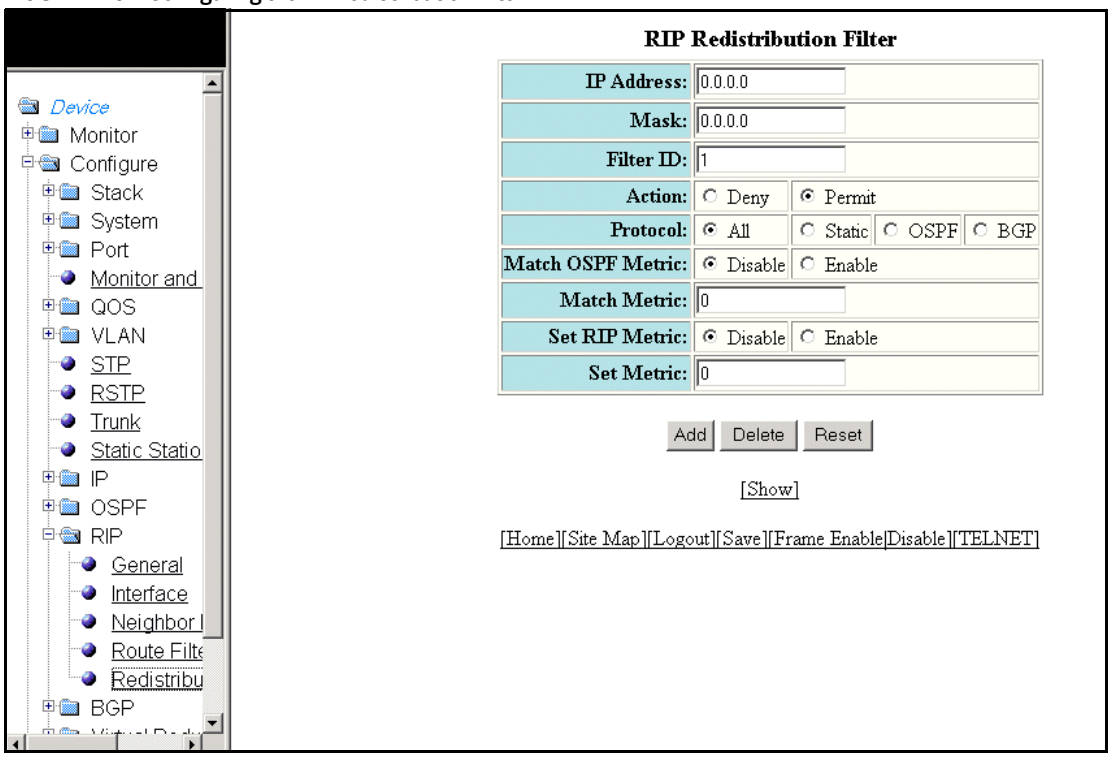
Configuring a RIP redistribution filter

To configure a RIP redistribution filter, perform the following steps.

1. Click **Configure** on the left pane and select **RIP**.
2. Click **Redistribution Filter**.

The **RIP Redistribution Filter** window is displayed as shown in Figure 179.

FIGURE 179 Configuring the RIP redistribution filter



3. Type a network IP address in the **IP Address** field.
4. Type an IP subnet mask in the **Mask** field.
5. Type a redistribution filter identifier in the **Filter ID** field.
6. Click **Deny** or **Permit** for **Action**.
7. Select one of the following options for **Protocol**:
   - **All** - Applies redistribution to all route types.
   - **Static** - Applies redistribution to IP static routes only.
   - **OSPF** - Applies redistribution to OSPF routes only.
   - **BGP** - Applies redistribution to BGP routes only.
8. Click **Disable** or **Enable** for **Set OSPF Metric**.
9. Type the match metric value from 1 through 15 in the **Match Metric** field. The match metric parameter applies the redistribution filter only to those routes with the specified metric value.
10. Click **Disable** or **Enable** for **Set RIP Metric**.

11. Type the RIP metric value in the **Set Metric** field.
12. Click **Add**.

The message **The change has been made** is displayed. To display the configured RIP redistribution filter, click **Show**.

To delete the configured RIP redistribution filter, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

28

Configuring PIM

In this chapter

- Configuring the general PIM settings 261
- Enabling a PIM interface 262

NOTE
The Protocol Independent Multicast (PIM) feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

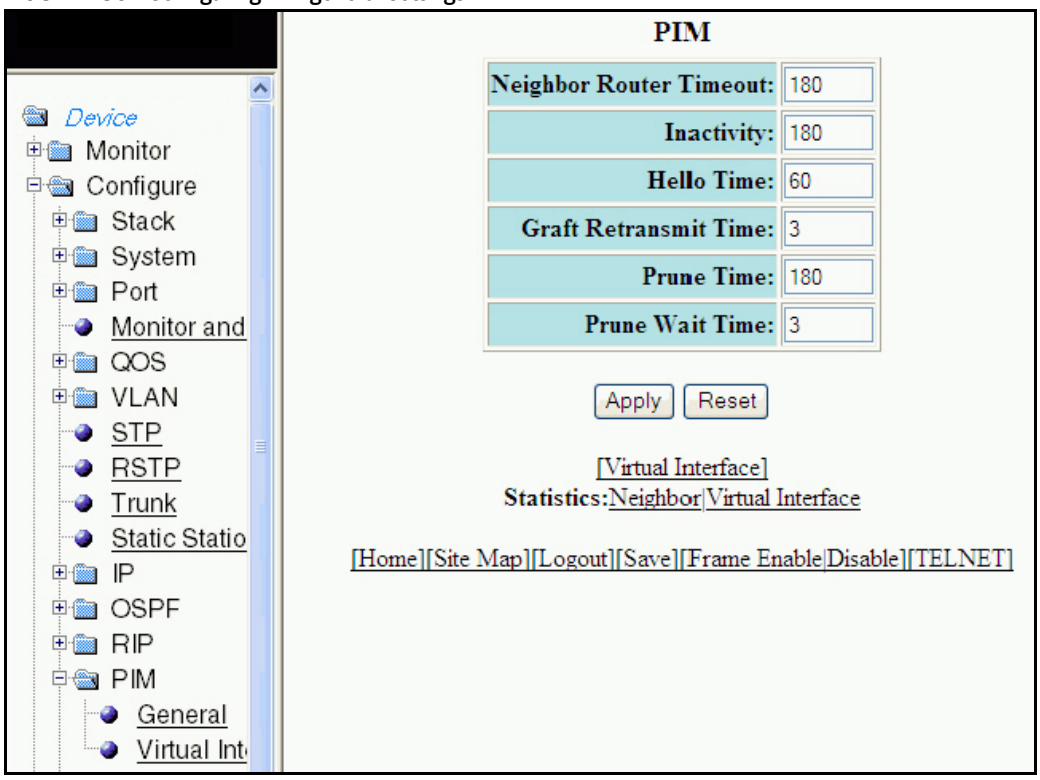
Configuring the general PIM settings

To modify the PIM general settings, perform the following steps.

1. Click **Configure** on the left pane and select **PIM**.
2. Click **General**.

The **PIM** window is displayed as shown in Figure 180.

FIGURE 180 Configuring PIM general settings



3. Type the neighbor timeout interval after which a PIM router considers a neighbor to be absent in the **Neighbor Router Timeout** field. The range is from 60 through 8000 seconds. The default is 180 seconds.
4. Type the number of seconds a forwarding entry can remain unused before the router deletes it in the **Inactivity** field. The range is from 10 through 3600 seconds. The default is 180 seconds.
5. Type the number of seconds between the transmission of hello packets to the PIM interfaces in the **Hello Time** field. The range is from 10 through 3600 seconds. The default is 60 seconds.
6. Type the number of seconds between the transmission of graft messages in the **Graft Retransmit Time** field. The range is from 2 through 10 seconds. The default is three seconds.
7. Type the interval at which periodic hello packets are sent to the PIM interfaces in the **Prune Time** field. The range is from 10 through 3600 seconds. The default is 180 seconds.
8. Type the amount of time a PIM router waits before stopping traffic to neighbor routers that do not want the traffic in the **Prune Wait Time** field. The range is from 0 through 3 seconds. The default is three seconds.
9. Click **Apply**.

To reset the data entered in the configuration pane, click **Reset**.

The **PIM** window provides links to configure and monitor PIM parameters:

- To configure a PIM interface, click **Virtual Interface**. For more information, refer to "Enabling a PIM interface" on page 262.
- To display information of the PIM neighbors, click **Neighbor**. For more information, refer to "Displaying the PIM neighbors" on page 89.
- To display information of the configured PIM interfaces, click **Virtual Interface**. For more information, refer to "Displaying the PIM virtual interface" on page 90.

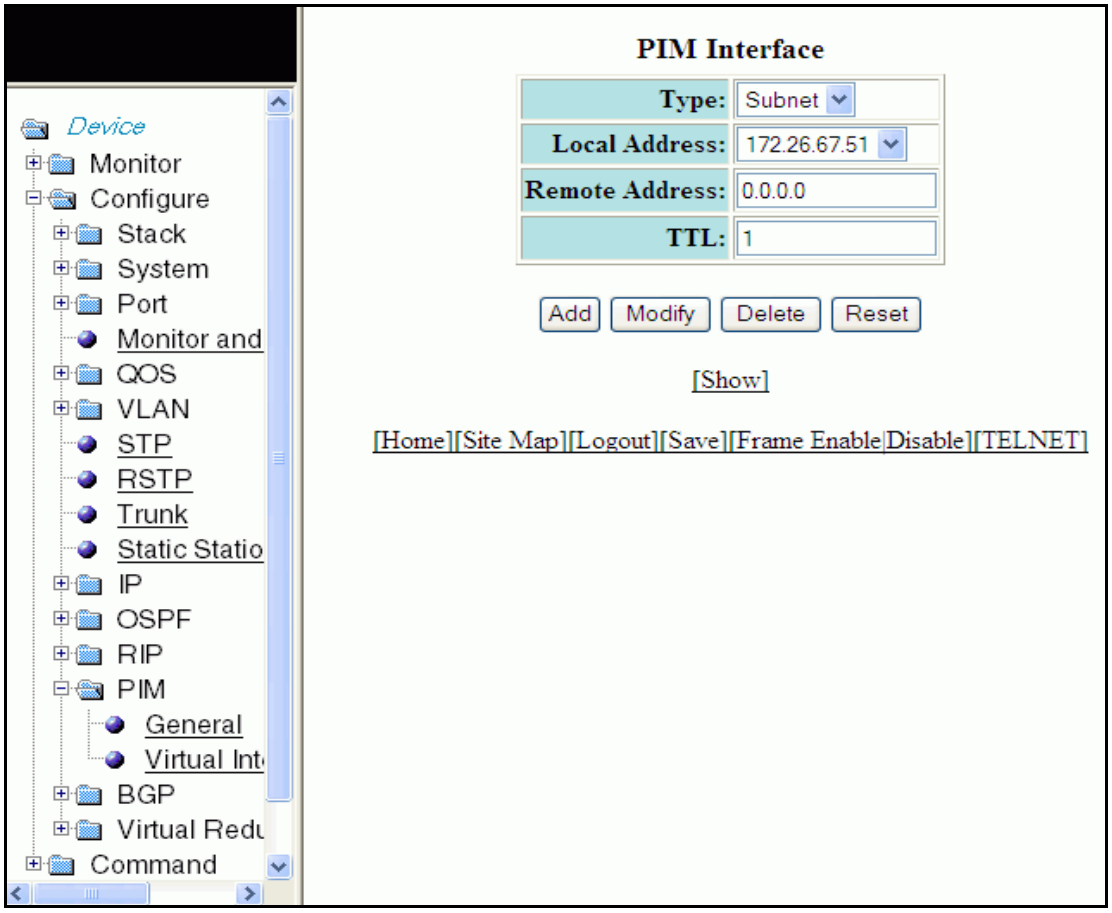
Enabling a PIM interface

To enable PIM interface, perform the following steps.

1. Click **Configure** on the left pane and select **PIM**.
2. Click **Virtual Interface**.

The **PIM Interface** window is displayed as shown in Figure 181.

FIGURE 181 Enabling PIM on a virtual interface



3. Select the type of the PIM interface in the **Type** list.
4. Select an IP address being configured on the interface in the **Local Address** list.
5. If you are configuring an IP tunnel interface, type the IP tunnel address of the destination interface (endpoint of the IP tunnel) in the **Remote Address** field.

NOTE
Make sure that IP tunneling is enabled on the destination router interface.

6. Type the minimum value required in a packet to be forwarded out of the interface in the **TTL** field. The range is from 1 through 31. The default Time-To-Live (TTL) value is one.
7. Click **Add**.

The message **The change has been made** is displayed and PIM is enabled on the interface. To display the configured PIM interface, click **Show**.

To modify the configured values of the PIM interface, click **Modify**. You can also delete the PIM interface by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

29

Configuring DVMRP

In this chapter

- Configuring the general DVMRP settings 265
- Configuring IGMP parameters 267
- Configuring a DVMRP interface 268

NOTE
The Distance Vector Multicast Routing Protocol (DVMRP) feature is specific to Brocade FSX devices running Layer 3 code. Brocade FCX and Brocade ICX 6610 devices do not support DVMRP.

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

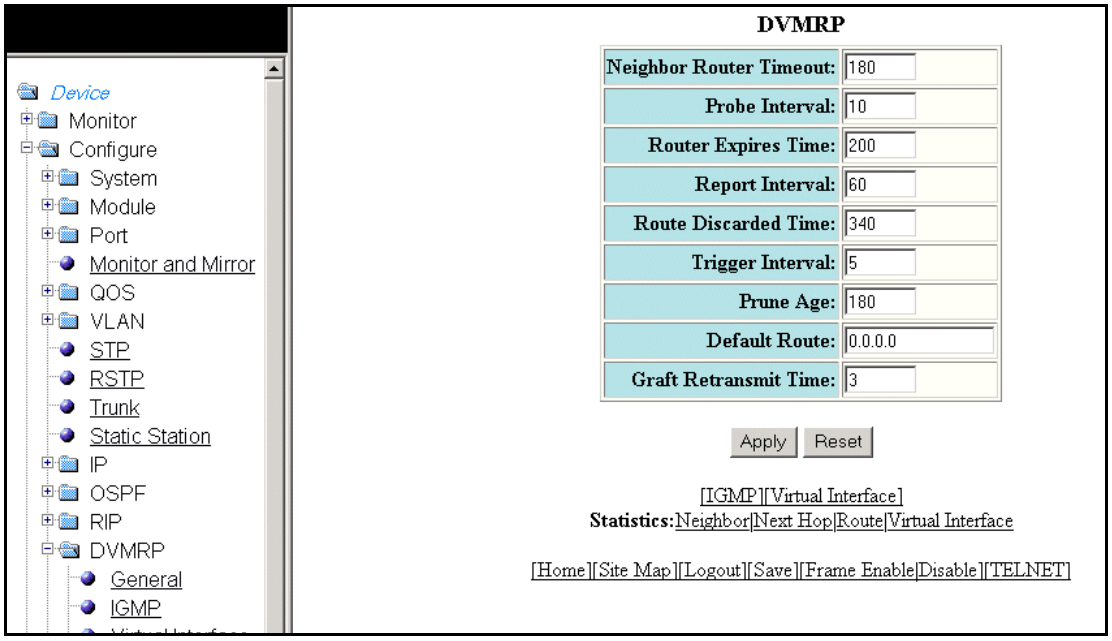
Configuring the general DVMRP settings

To configure the general DVMRP parameters, perform the following steps.

1. Click **Configure** on the left pane and select **DVMRP**.
2. Click **General**.

The **DVMRP** window is displayed as shown in Figure 182.

FIGURE 182 Configuring DVMRP general settings



3. Type the number of seconds the Layer 3 switch should wait before it defines an attached DVMRP neighbor Layer 3 switch as down, in the **Neighbor Router Timeout** field. The range is from 40 through 8000 seconds. The default value is 180 seconds.
4. Type the interval in which the neighbor probe messages should be sent to all DVMRP Layer 3 switches in the IP multicast group address, in the **Probe Interval** field.
5. Type the number of seconds a route is considered valid in the absence of the next route update in the **Router Expires Time** field. The range is from 20 through 4000 seconds. The default value is 200 seconds.
6. Type the number of seconds the Layer 3 switches propagate their complete routing tables to other neighbor DVMRP routers in the **Report Interval** field. The range is from 10 through 2000 seconds. The default value is 60 seconds.
7. Type the period of time before a route is deleted in the **Route Discard Time** field. The range is from 40 through 8000 seconds. The default value is 340 seconds.
8. Type the number of seconds the trigger updates (contains changes in the network topology) are sent, in the **Trigger Interval** field. The range is from 5 through 30 seconds. The default value is five seconds.
9. Type the number of seconds a prune state remains in effect for a source-routed multicast tree, in the **Prune Age** field. The range is from 20 through 3600 seconds. The default value is 180 seconds.
10. Type the IP address of the default gateway for DVMRP in the **Default Route** field.
11. Type the number of seconds that a Layer 3 switch sending a graft message waits for a graft acknowledgement from an upstream Layer 3 switch before retransmitting that message, in the **Graft Retransmit Time** field. The range is from 5 through 3600 seconds. The default value is 10 seconds.
12. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

The **DVMRP** window links to monitor DVMRP parameters:

- Click **IGMP** to configure the Internet Group Management Protocol (IGMP) parameters. For more information, refer to "Configuring IGMP parameters" on page 267.
- Click **Virtual Interface** to configure a DVMRP Interface. For more information, refer to "Configuring a DVMRP interface" on page 268.
- The **Statistics** links can be used to monitor the DVMRP parameters:
  - To display the DVMRP neighbors information, click **Neighbor**. For more information, refer to "Displaying DVMRP neighbors" on page 93.
  - To display the DVMRP next hop information, click **Next Hop**. For more information, refer to "Displaying DVMRP next hop entries" on page 94.
  - To display the DVMRP route information, click **Route**. For more information, refer to "Displaying DVMRP routes" on page 95.
  - To display the DVMRP virtual interface information, click **Virtual Interface**. For more information, refer to "Displaying DVMRP virtual interfaces" on page 96.

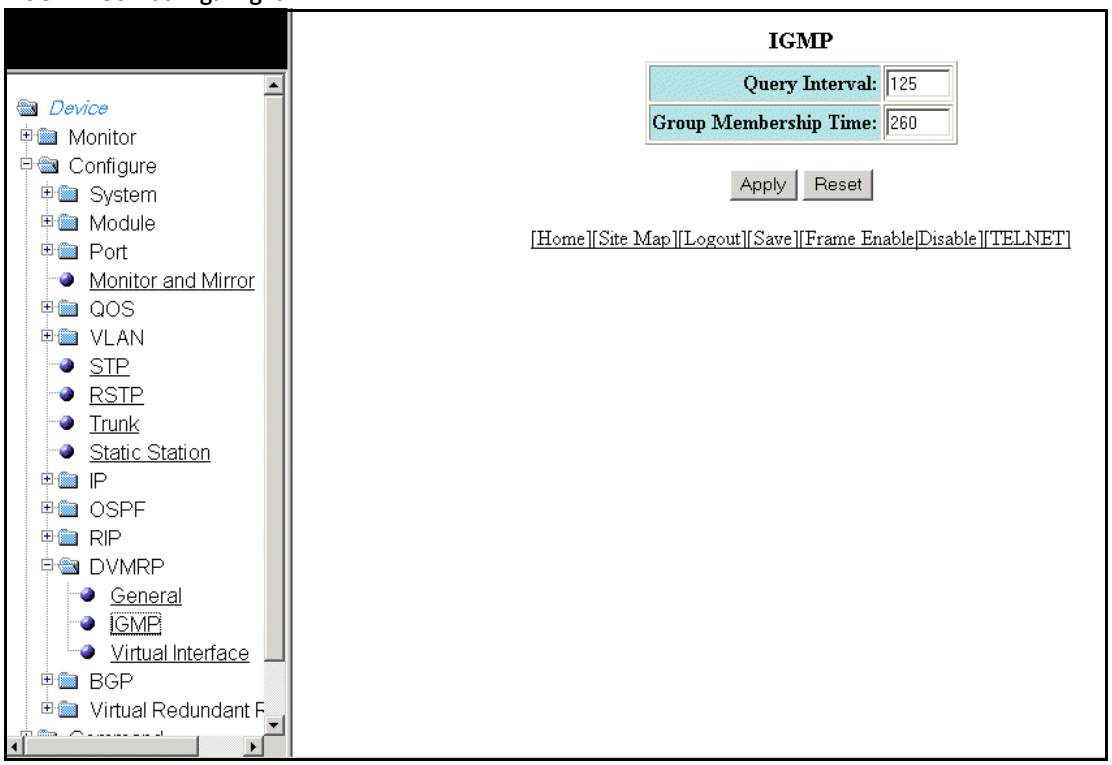
Configuring IGMP parameters

To configure Internet Group Management Protocol (IGMP), perform the following steps.

1. Click **Configure** on the left pane and select **DVMRP**.
2. Click **IGMP**.

The **IGMP** window is displayed as shown in Figure 183.

FIGURE 183 Configuring IGMP



3. Type an IGMP query interval in the **Query Interval** field. The range is from 10 through 3600 seconds. The default is 125 seconds.

   The IGMP query interval period defines how often a Layer 3 switch will query an interface for group membership.

4. Type a group membership interval in the **Group Membership Time** field. The range is from 20 through 7200 seconds. The default is 260 seconds.

   Group membership time defines how long a group remains active on an interface in the absence of a group report.

5. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

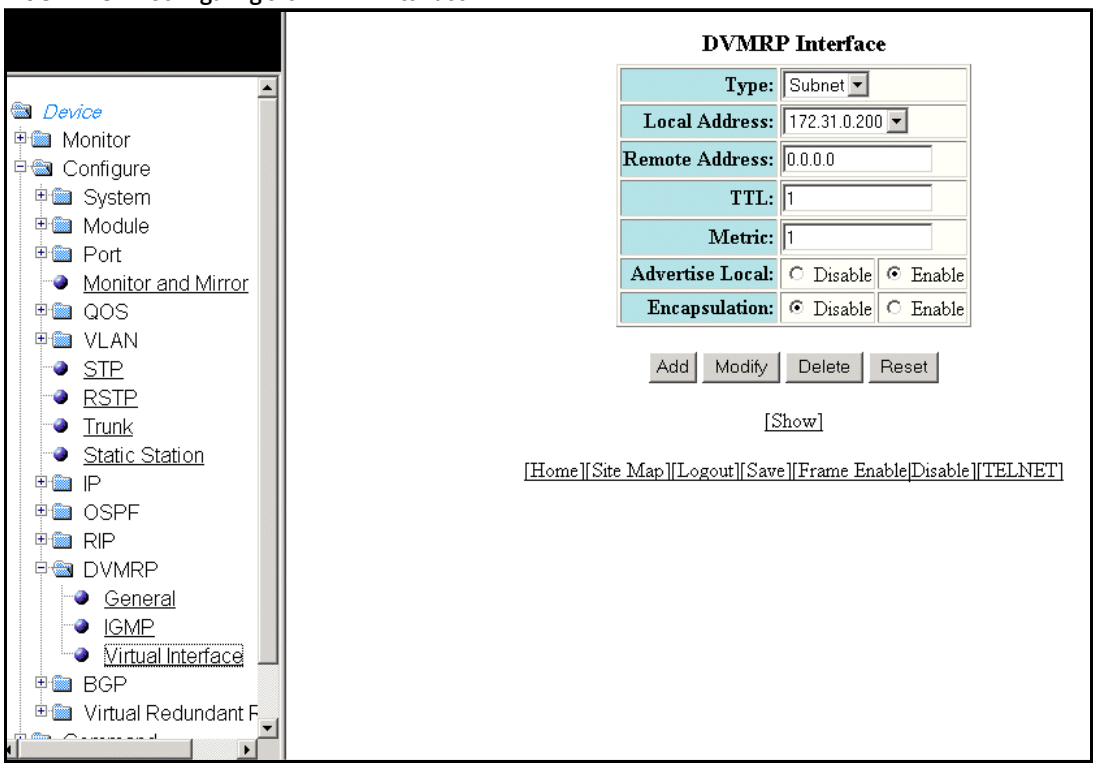
Configuring a DVMRP interface

To configure a DVMRP interface, perform the following steps.

1. Click **Configure** on the left pane and select **DVMRP**.
2. Click **Virtual Interface**.

The **DVMRP Interface** window is displayed as shown in Figure 184.

FIGURE 184 Configuring the DVMRP interface



3. Select a type of the DVMRP interface in the **Type** list.
4. Select an IP address to be configured on the interface in the **Local Address** list.
5. Type the minimum value required in a packet in order to be forwarded out of the interface in the **TTL** field. The range is from 1 through 64. The default value is one.
6. Type a metric that a Layer 3 switch uses when establishing reverse paths to some networks on directly attached interfaces, in the **Metric** field. The range is from 1 through 31 hops. The default is one hop.
7. Click **Disable** or **Enable** for **Advertise Local**. By default, the advertisement of a local route on the interface is enabled.
8. Click **Disable** or **Enable** for **Encapsulation**.
9. Click **Add**.

The message **The change has been made** is displayed and the DVMRP interface is configured. To display the configured DVMRP interface, click **Show**.

To modify the configured values of the DVMRP interface, click **Modify**. To delete the DVMRP interface, click **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Chapter

Configuring BGP 30

In this chapter

- Configuring the general BGP settings 271
- Configuring a BGP address filter 273
- Configuring a BGP aggregate address 274
- Configuring a BGP AS-path filter 276
- Configuring a BGP community filter 277
- Configuring a BGP neighbor 278
- Configuring a BGP network 284
- Configuring BGP redistribute parameters 285
- Configuring a BGP route map filter 286

NOTE
The Border Gateway Protocol (BGP) feature is specific to Brocade FCX, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code.

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

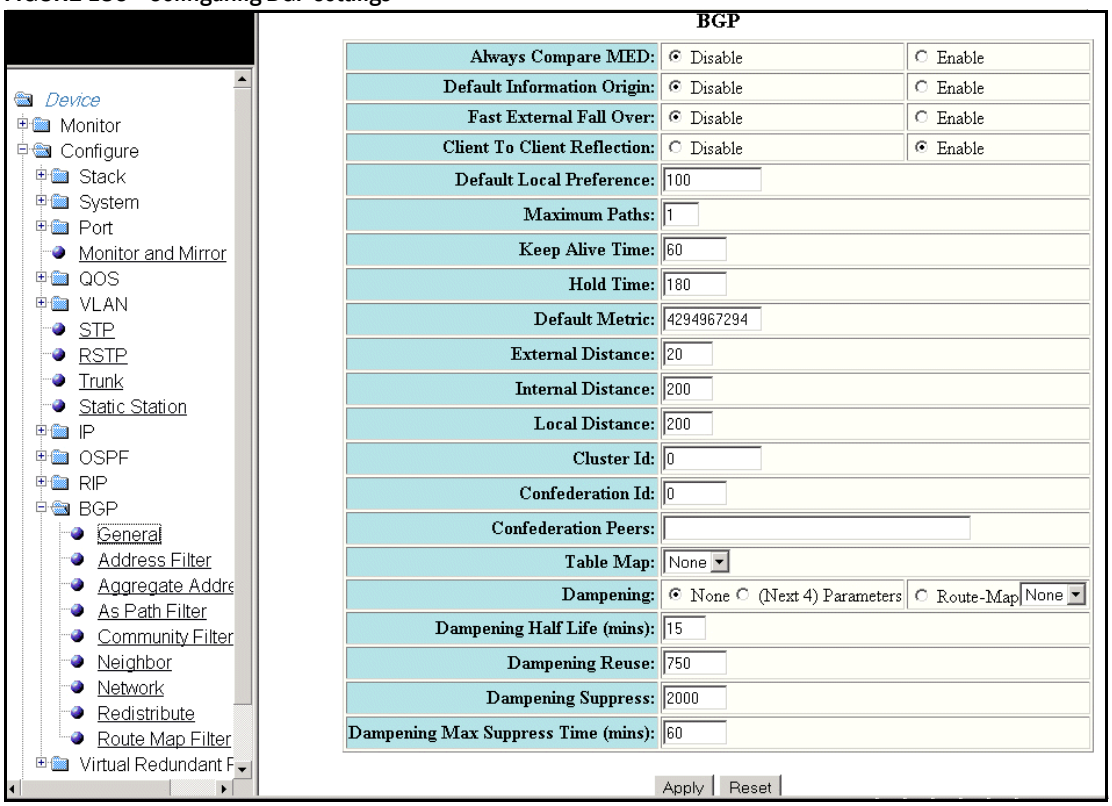
Configuring the general BGP settings

To configure BGP general settings, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **General**.

The **BGP** window is displayed as shown in Figure 185.

FIGURE 185 Configuring BGP settings



3. Click **Disable** or **Enable** for **Always Compare MED**. If you click **Enable**, the Layer 3 switch will always compare MEDs. A Multi-Exit Discriminator (MED) is a value that the BGP algorithm uses when comparing multiple paths received from different BGP neighbors in the same Autonomous System (AS) for the same route.
4. Click **Disable** or **Enable** for **Default Information Origin**. If you click **Enable**, the Layer 3 switch originates and advertise a default route using BGP.
5. Click **Disable** or **Enable** for **Fast External Fall Over**. If you click **Enable**, the Layer 3 switch will immediately close the BGP session and the TCP connection to the locally attached neighbors that die.
6. Click **Disable** or **Enable** for **Client To Client Reflection**. If you click **Disable**, the route reflection between clients is disabled.
7. Type the preference from 0 through 4294967295 in the **Default Local Preference** field. The default local preference is 100.
8. Type the maximum number of shared paths from 2 through 4 in the **Maximum Paths** field. The default is one.
9. Type how often the Layer 3 switch should send keepalive messages to the neighbor in the **Keep Alive Time** field. The range is from 0 through 65535 seconds. The default is 60 seconds.
10. Type how long the Layer 3 switch must wait for a keepalive or update message from a neighbor before concluding that the neighbor is dead in the **Hold Time** field. The range is 0 and 3 through 65535 (one and two are not allowed).
11. Type the metric from 0 through 4294967295 in the **Default Metric** field.

12. Type the Exterior Border Gateway Protocol (EBGP) distance from 1 through 255 in the **External Distance** field.
13. Type the Interior Gateway Protocol (IBGP) distance from 1 through 255 in the **Internal Distance** field.
14. Type the local BGP distance from 1 through 255 in the **Local Distance** field.
15. Type the cluster identifier number from 0 through 4294967295 in the **Cluster Id** field.
16. Type the confederation number from 0 through 65535 in the **Confederation Id** field.
17. Type the sub-AS number for the sub-autonomous systems in the confederation from 1 through 65535 in the **Confederation Peers** field.
18. Select a table map in the **Table Map** list.
19. Click one of the following options for **Dampening**:
    - **None**
    - **(Next 4) Parameters**
    - **Route-Map**

      If you click **Route-Map**, select a route map in the list.
20. Type the half life time, which is the number of minutes after which the route penalty becomes half its value, in the **Dampening Half Life (mins)** field. The range is from 1 through 45 minutes. The default is 15 minutes.
21. Type the reuse threshold, which is the minimum penalty a route can have and still be suppressed by the Layer 3 switch, in the **Dampening Reuse** field. The range is from 1 through 20000. The default is 750.
22. Type the suppression threshold, which is the penalty value at which the Layer 3 switch stops using the route, in the **Dampening Suppress** field. The range is from 1 through 20000. The default is 2000.
23. Type the maximum suppression time, which is the maximum number of minutes a route can be suppressed regardless of how unstable the route has been before this time, in the **Dampening Max Suppress Time (mins)** field. The range is from 1 through 20000 minutes. The default is four times the half-life, for example, 60 minutes.
24. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

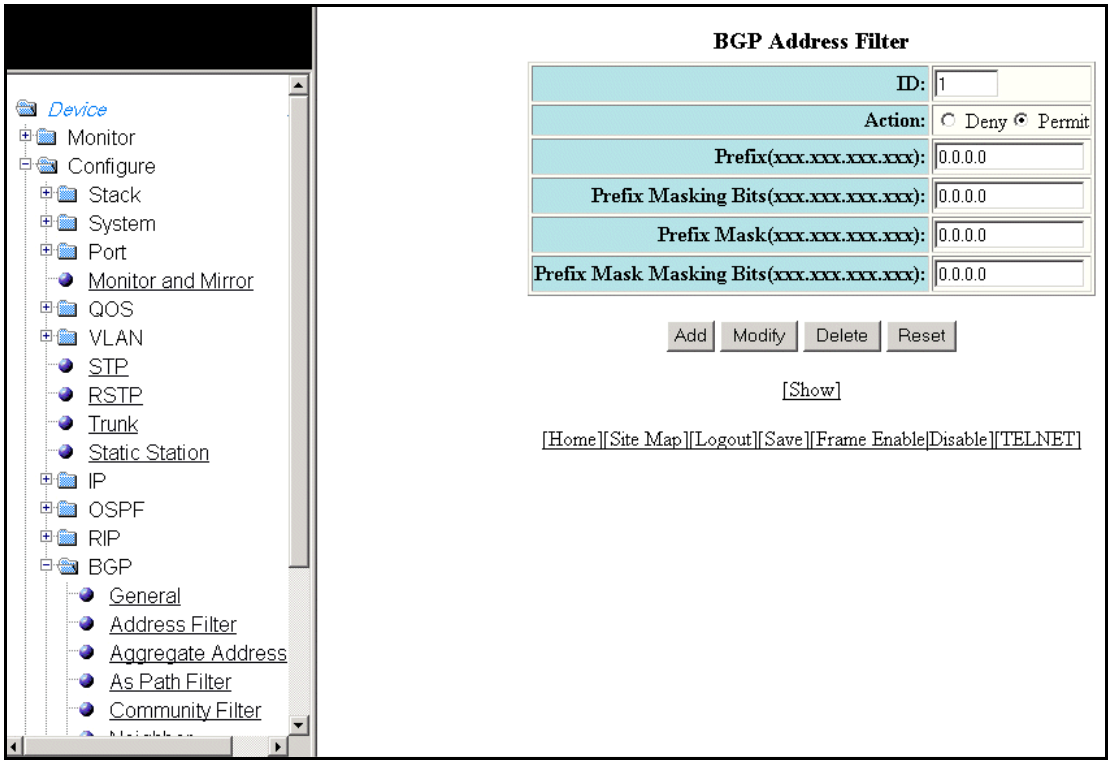
Configuring a BGP address filter

To configure the Layer 3 switch to explicitly permit or deny specific IP addresses received in updates from BGP neighbors, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Address Filter**.

The **BGP Address Filter** window is displayed as shown in Figure 186.

FIGURE 186 Configuring the BGP address filter



3. Type a filter number in the **ID** field.
4. Click **Deny** or **Permit** for **Action** so that the Layer 3 switch denies or permits the route into the BGP table if the filter match is true.
5. Type the prefix in xxx.xxx.xxx.xxx format in the **Prefix** field.
6. Type the prefix masking bits in xxx.xxx.xxx.xxx format in the **Prefix Masking Bits** field.
7. Type the prefix mask in xxx.xxx.xxx.xxx format in the **Prefix Mask** field.
8. Type the prefix mask masking bits in xxx.xxx.xxx.xxx format in the **Prefix Mask Masking Bits** field.
9. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP address filter, click **Show**.

To modify the configured BGP address filter, click **Modify**. You can also delete the BGP address filter by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

Configuring a BGP aggregate address

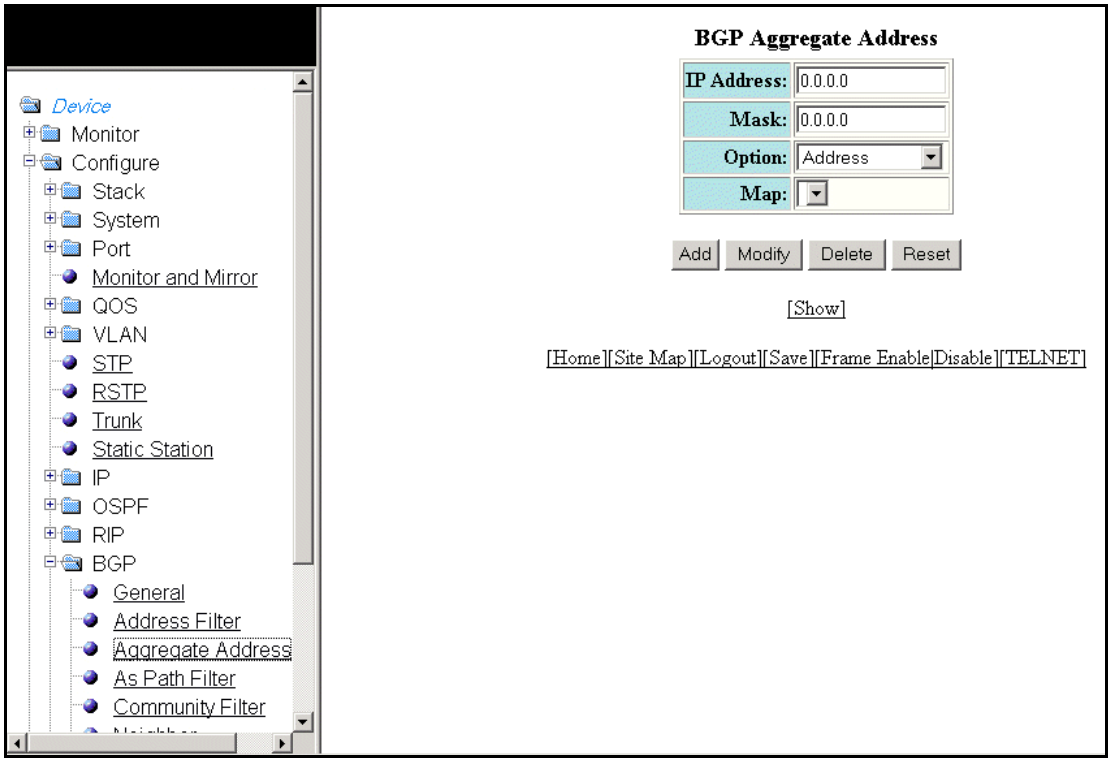
By default, the Layer 3 switch advertises individual routes for all the networks. The aggregation feature allows you to configure the Layer 3 switch to aggregate routes in a range of networks into a single Classless Interdomain Routing (CIDR) number.

To configure a BGP aggregate address, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Aggregate Address**.

The **BGP Aggregate Address** window is displayed as shown in Figure 187.

FIGURE 187 Configuring the BGP aggregate address



3. Type the IP address of the device in the **IP Address** field.
4. Type the network mask in the **Mask** field.
5. Select one of the following options in the **Option** list:
   - **Address**
   - **As Set** - The Layer 3 switch aggregates AS-path information for all the routes in the aggregate address into a single AS-path.
   - **Summary Only** - The Layer 3 switch does not advertise more specific routes contained within the aggregate route.
   - **Suppress Map** - The more specific routes contained in the specified route map will be prevented from being advertised.
   - **Advertise Map** - The Layer 3 switch will be configured to advertise the more specific routes in the specified route map.
   - **Attribute Map** - The Layer 3 switch will be configured to set attributes for the aggregate routes based on the specified route map.
6. Select a route map name in the **Map** list.
7. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP aggregate address, click **Show**.

To modify the configured BGP aggregate address, click **Modify**. You can also delete the BGP aggregate address by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

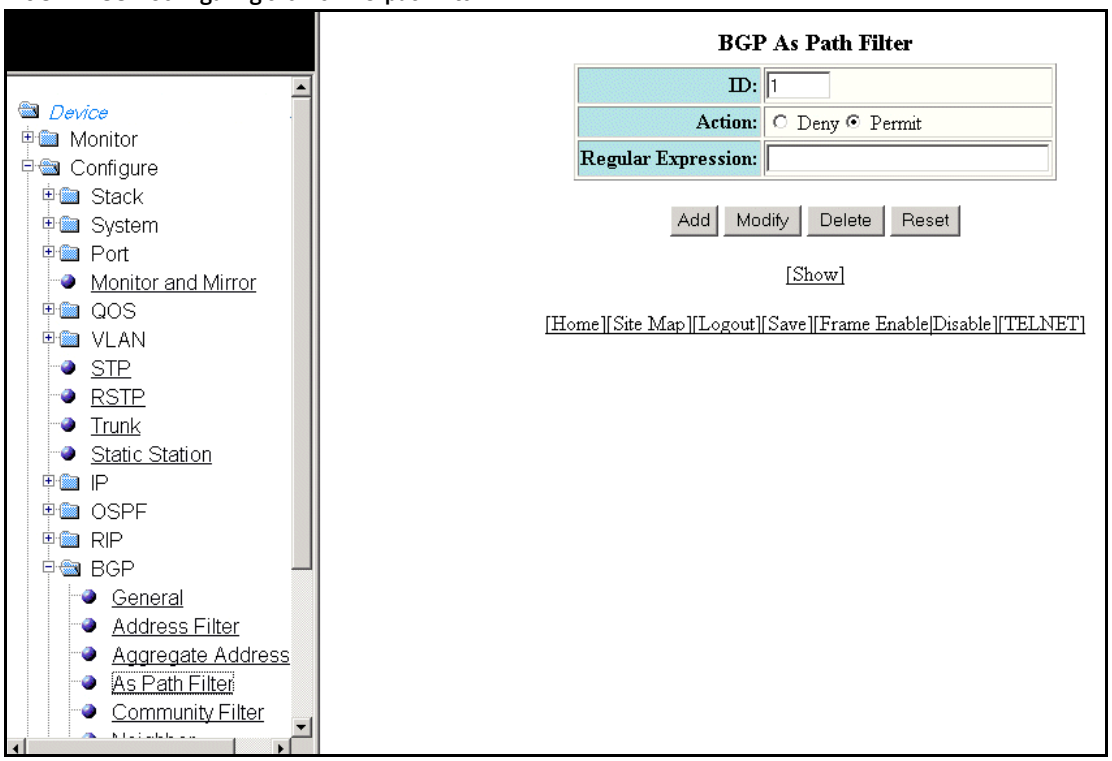
Configuring a BGP AS-path filter

To configure a BGP AS-path filter, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **As Path Filter**.

The **BGP As Path Filter** window is displayed as shown in Figure 188.

FIGURE 188 Configuring the BGP AS-path filter



3. Type an AS-path filter identifier from 1 through 100 in the **ID** field.
4. Click **Deny** or **Permit** for **Action** so that the Layer 3 switch can deny or permit the route into the BGP table when the filter match is true.
5. Type an exact AS-path string if you want to filter for a specific value or type regular expressions in the filter string in the **Regular Expression** field.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured AS-path filter, click **Show**.

To modify the configured BGP AS-path filter, click **Modify**. You can also delete the BGP AS-path filter by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

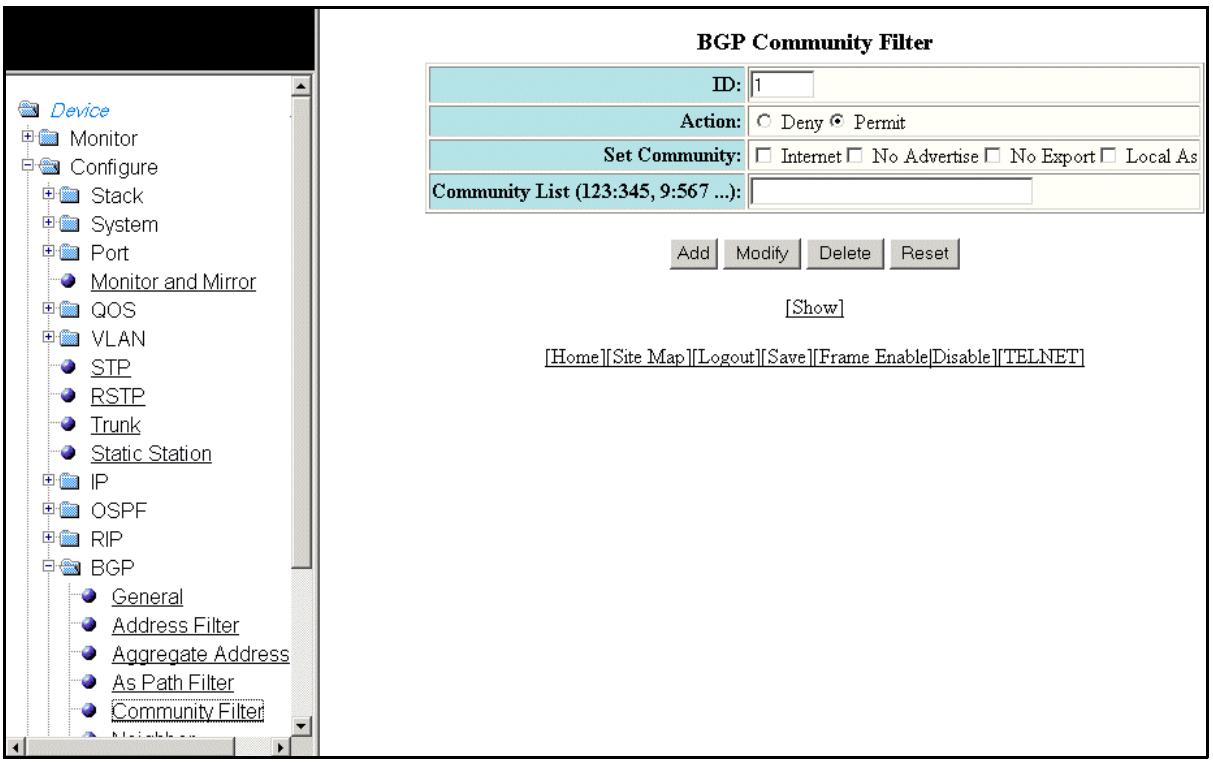
Configuring a BGP community filter

To configure a BGP community filter, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Community Filter**.

The **BGP Community Filter** window is displayed as shown in Figure 189.

FIGURE 189 Configuring the BGP community filter



3. Type a community path filter identifier from 1 through 100 in the **ID** field.
4. Click **Deny** or **Permit** for **Action** so that the Layer 3 switch denies or permits the route into the BGP table if the filter match is true.
5. Select one the following options for **Set Community**:
   - **Internet** - Checks for routes that do not have the community attribute. By default, routes without a specific community are considered to be the members of the largest community, the Internet.
   - **No Advertise** - Filters the routes with the community NO_ADVERTISE. A route in this community should not be advertised to any BGP neighbors.

- **No Export** - Filters for routes with the community NO_EXPORT. A route in this community should not be advertised to any BGP neighbors outside the local AS. If the Layer 3 switch is a member of a confederation, the Layer 3 switch advertises the route only within the confederation.
- **Local As** - Checks for routes with the community LOCAL_AS. This community applies only to confederations. The Layer 3 switch advertises the route only within the sub-AS.

6. Type a specific community number to filter in *num*:*num* format in the **Community List** field. You can enter up to 20 community numbers within the same field.
7. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP community filter, click **Show**.

To modify the configured BGP community filter, click **Modify**. You can also delete the BGP community filter by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

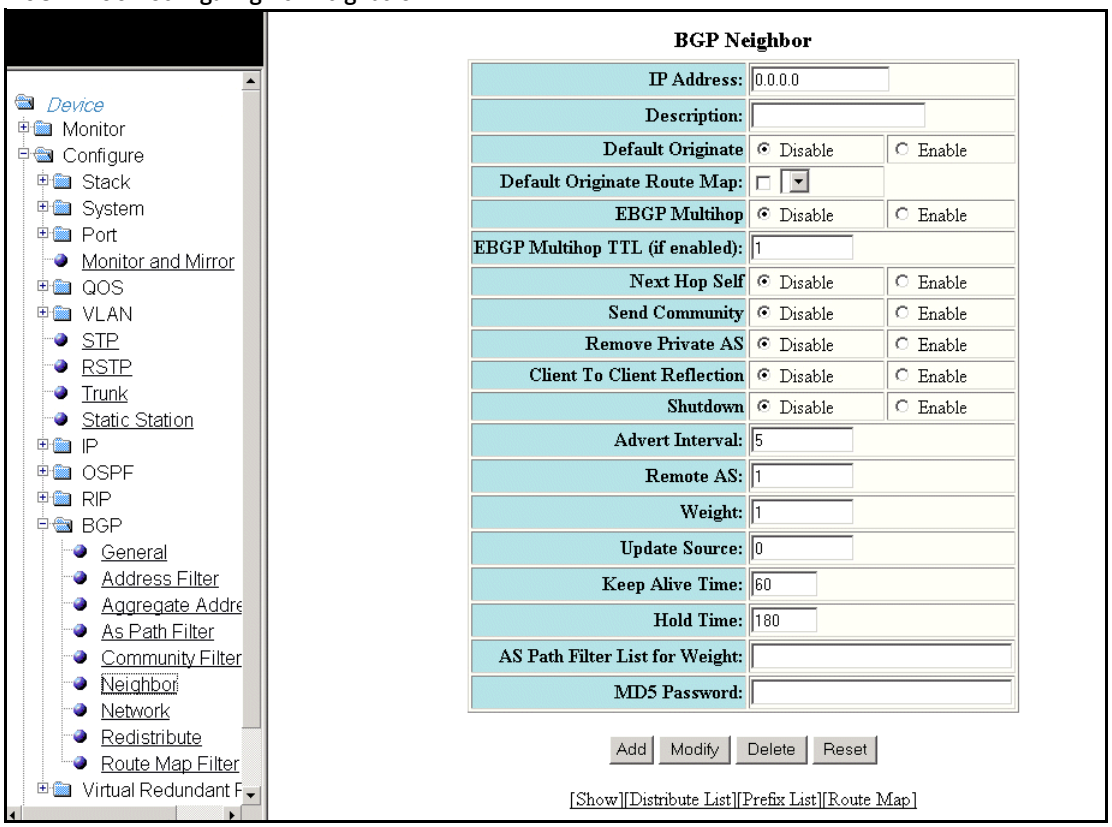
Configuring a BGP neighbor

To configure a BGP neighbor, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Neighbor**.

The **BGP Neighbor** window is displayed as shown in Figure 190.

FIGURE 190 Configuring BGP neighbors



3. Type the IP address of the neighbor in the **IP Address** field.
4. Type a name for the neighbor in the **Description** field.
5. Click **Disable** or **Enable** for **Default Originate**. If you click **Enable**, the Layer 3 switch sends the default route 0.0.0.0 to the neighbor.
6. Select the **Default Originate Route Map** check box and select a route map in the list. The route map injects the default route conditionally, based on the match conditions in the route map.
7. Click **Disable** or **Enable** for **EBGP Multihop**.
8. Type the time-to-live interval for the neighbor from 0 through 255 in the **EBGP Multihop TTL** field, if you have clicked **Enable** for **EBGP Multihop**. The default is zero.
9. Click **Disable** or **Enable** for **Next Hop Self**. If you click **Enable**, the Layer 3 switch will list itself as the next hop in updates sent to the specified neighbor.
10. Click **Disable** or **Enable** for **Send Community**. If you click **Enable**, the Layer 3 switch sends the community attribute updates to the specified neighbor.
11. Click **Disable** or **Enable** for **Remove Private AS**. If you click **Enable**, the Layer 3 switch will remove private AS numbers from the update messages the Layer 3 switch sends to this neighbor.
12. Click **Disable** or **Enable** for **Client To Client Reflection**. If you click **Enable**, the neighbor becomes a route-reflector client of the Layer 3 switch.
13. Click **Disable** or **Enable** for **Shutdown**. If you click **Enable**, the session with this neighbor will be administratively shut down.
14. Type an advertisement interval, which is the minimum delay (in seconds) between messages to the specified neighbor, in the **Advert Interval** field. The range is from 0 through 600. The default is 30 for EBGP neighbors (neighbors in other ASes). The default is five for IBGP neighbors (neighbors in the same AS).
15. Type the AS the remote neighbor belongs to in the **Remote AS** field. The range is from 1 through 65535. There is no default value.
16. Type the weight that the Layer 3 switch adds to routes received from the specified neighbor in the **Weight** field. The default weight is zero. BGP prefers larger weights over smaller weights.
17. Type an interface through which the Layer 3 switch can communicate with the neighbor in the **Update Source** field.
18. Type the keepalive interval from 0 through 65535 seconds in the **Keep Alive Time** field.
19. Type the hold interval from 0 or 3 through 65535 seconds (1 and 2 are not allowed) in the **Hold Time** field.
20. Type an AS-path filter list or a list of AS-path ACLs in the **AS Path Filter List for Weight** field.
21. Type a string, which can be up to 80 characters long, in the **MD5 Password** field.
22. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP neighbor, click **Show**.

To modify the configured BGP neighbor, click **Modify**. You can also delete the BGP neighbor by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **BGP Neighbor** window contains the following links:

- To configure a BGP neighbor distribute list, click **Distribute List**. For more information, refer to "Configuring a BGP distribute list" on page 280.
- To configure a BGP neighbor prefix list, click **Prefix List**. For more information, refer to "Configuring a BGP prefix list" on page 282.
- To configure a BGP neighbor route map, click **Route Map**. For more information, refer to "Configuring a BGP route map" on page 283.

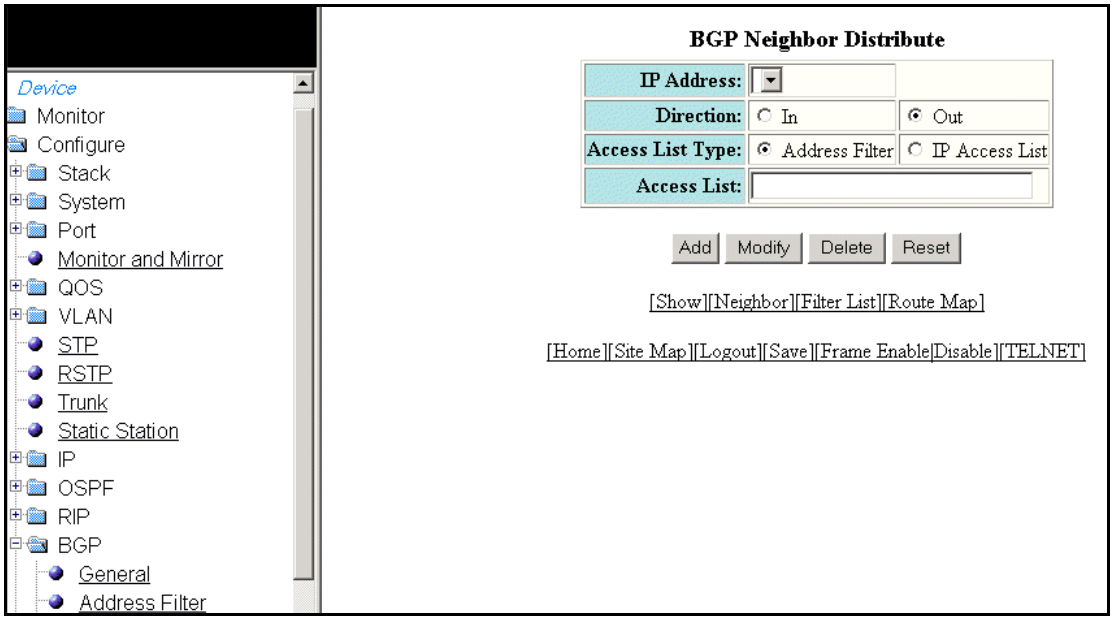
Configuring a BGP distribute list

A neighbor distribute list is a list of BGP address filters or ACLs that filter the traffic to or from a neighbor. To configure a BGP neighbor distribute list, perform the following steps.

1. Click **Distribute List** on the **BGP Neighbor** window.

The **BGP Neighbor Distribute** window is displayed as shown in Figure 191.

FIGURE 191 Configuring the BGP neighbor distribute list



2. Select an IP address of the neighbor in the **IP Address** list.
3. Click **In** or **Out** for **Direction** so that the distribute list applies to inbound or outbound routes respectively.
4. Click **Address Filter** or **IP Access List** for **Access List Type**.
5. Type the name or number of a standard, extended, or named ACL in the **Access List** field.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured neighbor distribute list, click **Show**.

To modify the configured neighbor distribute list, click **Modify**. You can also delete the neighbor distribute list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **BGP Neighbor Distribute** window contains the following links:

- To configure a BGP neighbor, click **Neighbor**. For more information, refer to "Configuring a BGP neighbor" on page 278.
- To configure a BGP neighbor filter list, click **Filter List**. For more information, refer to "Configuring a BGP filter list" on page 281.
- To configure a BGP neighbor route map, click **Route Map**. For more information, refer to "Configuring a BGP route map" on page 283.

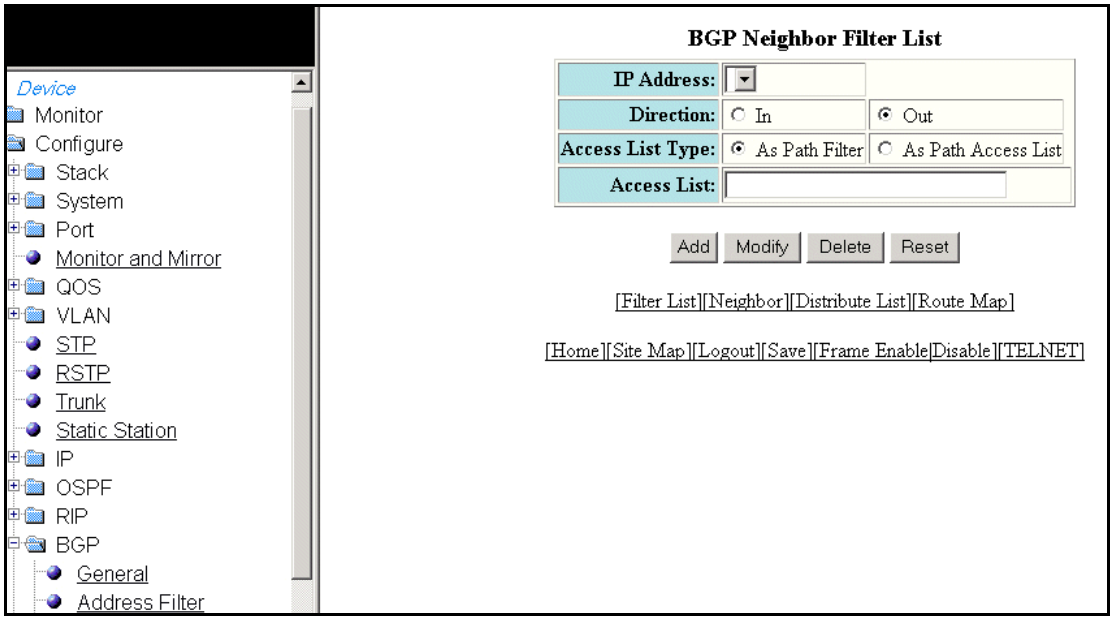
Configuring a BGP filter list

The neighbor filters allow you to specify the neighbor Layer 3 switches from which the Brocade device can receive BGP routes.To configure a BGP neighbor filter list, perform the following steps.

1. Click **Filter List** on the **BGP Neighbor Distribute** window.

The **BGP Neighbor Filter List** window is displayed as shown in Figure 192.

FIGURE 192 Configuring the BGP neighbor filter list



2. Select an IP address of the neighbor in the **IP Address** list.
3. Click **In** or **Out** for **Direction** so that the filter list applies to inbound or outbound routes respectively.
4. Click **As Path Filter** or **As Path Access List** for **Access List Type**.
5. Type the name or number of a standard, extended, or named ACL in the **Access List** field.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP neighbor filter list, click **Show**.

To modify the configured BGP neighbor filter list, click **Modify**. You can also delete the BGP neighbor filter list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **BGP Neighbor Filter List** window contains the following links:

- To configure a BGP neighbor, click **Neighbor**. For more information, refer to "Configuring a BGP neighbor" on page 278.
- To configure a BGP neighbor distribute list, click **Distribute List**. For more information, refer to "Configuring a BGP distribute list" on page 280.
- To configure a BGP neighbor route map, click **Route Map**. For more information, refer to "Configuring a BGP route map" on page 283.

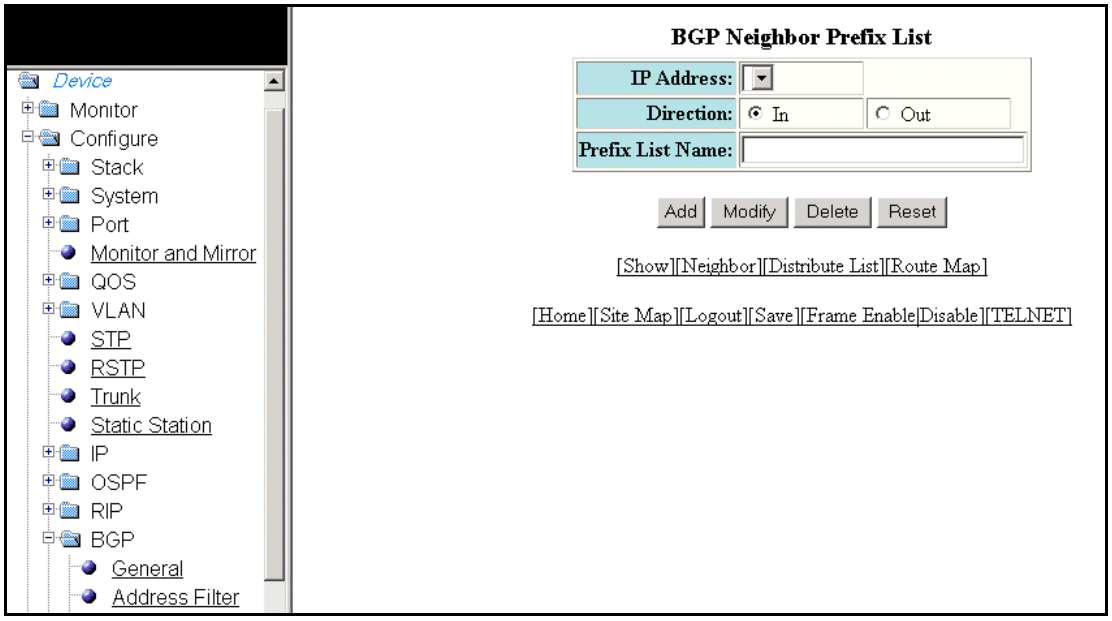
Configuring a BGP prefix list

To configure a BGP neighbor prefix list, perform the following steps.

1. Click **Prefix List** on the **BGP Neighbor** window.

The **BGP Neighbor Prefix List** window is displayed as shown in Figure 193.

FIGURE 193 Configuring the BGP neighbor prefix list



2. Select an IP address of the neighbor in the **IP Address** list.
3. Click **In** or **Out** for **Direction** so that the prefix list applies to inbound or outbound routes respectively.
4. Type a text string describing the prefix list in the **Prefix List Name** field.
5. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP neighbor prefix list, click **Show**.

To modify the configured BGP neighbor prefix list, click **Modify**. You can also delete the BGP neighbor prefix list by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **BGP Neighbor Prefix List** window contains the following links:

- To configure a BGP neighbor, click **Neighbor**. For more information, refer to "Configuring a BGP neighbor" on page 278.
- To configure a BGP neighbor distribute list, click **Distribute List**. For more information, refer to "Configuring a BGP distribute list" on page 280.
- To configure a BGP neighbor route map, click **Route Map**. For more information, refer to "Configuring a BGP route map" on page 283.

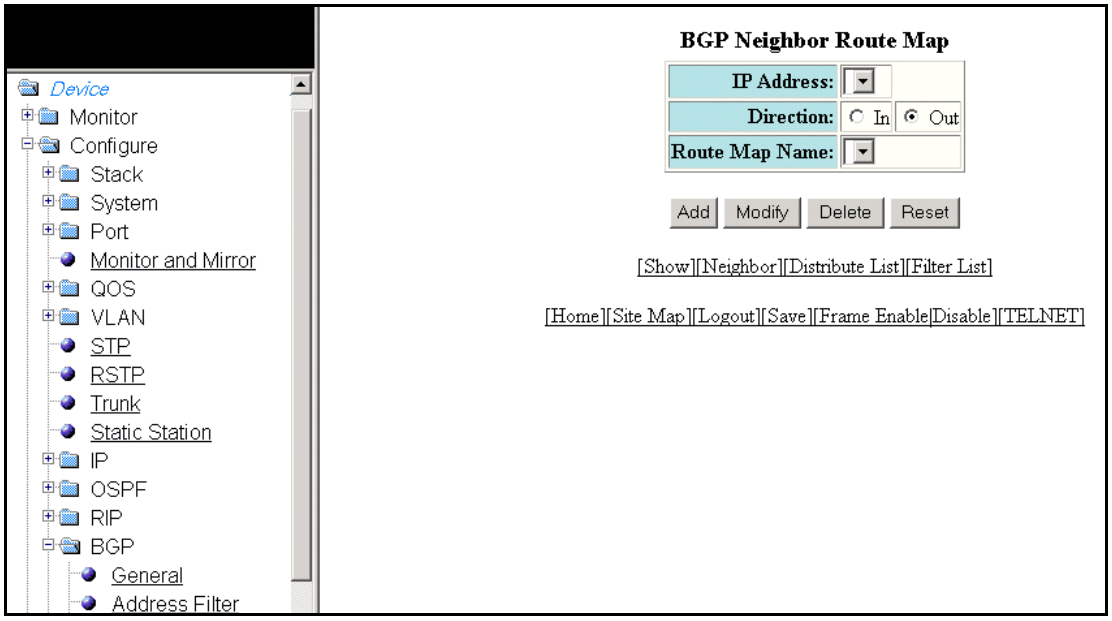
Configuring a BGP route map

To configure a BGP neighbor route map, perform the following steps.

1. Click **Route Map** on the **BGP Neighbor** window.

The **BGP Neighbor Route Map** window is displayed as shown in Figure 194.

FIGURE 194 Configuring the BGP neighbor route map



2. Select an IP address of the neighbor in the **IP Address** list.
3. Click **In** or **Out** for **Direction** so that the route map applies to inbound or outbound routes respectively.
4. Select a route map in the **Route Map Name** list.

The message **The change has been made** is displayed. To display the configured BGP neighbor route map, click **Show**.

To modify the configured BGP neighbor route map, click **Modify**. You can also delete the BGP neighbor route map by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **BGP Neighbor Route Map** window contains the following links:

- To configure a BGP neighbor, click **Neighbor**. For more information, refer to "Configuring a BGP neighbor" on page 278.
- To configure a BGP neighbor distribute list, click **Distribute List**. For more information, refer to "Configuring a BGP distribute list" on page 280.
- To configure a BGP neighbor filter list, click **Filter List**. For more information, refer to "Configuring a BGP filter list" on page 281.

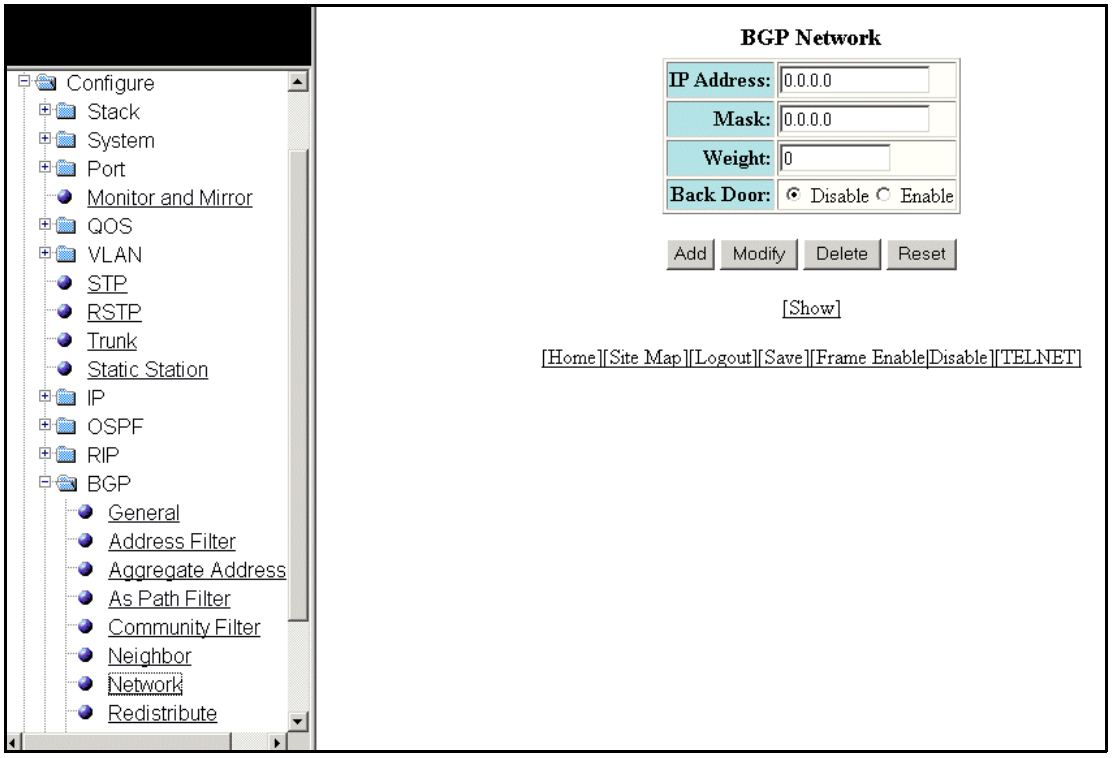
Configuring a BGP network

To configure a BGP network, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Network**.

The **BGP Network** window is displayed as shown in Figure 195.

FIGURE 195 Configuring the BGP network



3. Type the network IP address in the **IP Address** field.
4. Type the network mask in the **Mask** field.
5. Type the weight to be added to routes to this network in the **Weight** field.

6. Click **Disable** or **Enable** for **Back Door**.

   The **Back Door** parameter changes the administrative distance of the route to this network from the EBGP administrative distance (20 by default) to the Local BGP weight (200 by default), thus tagging the route as a back door route. Enable this parameter if you want the Layer 3 switch to prefer IGP routes such as RIP or OSPF routes over the EBGP route for the network.

7. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP network, click **Show**.

To modify the configured BGP network, click **Modify**. You can also delete the BGP network by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

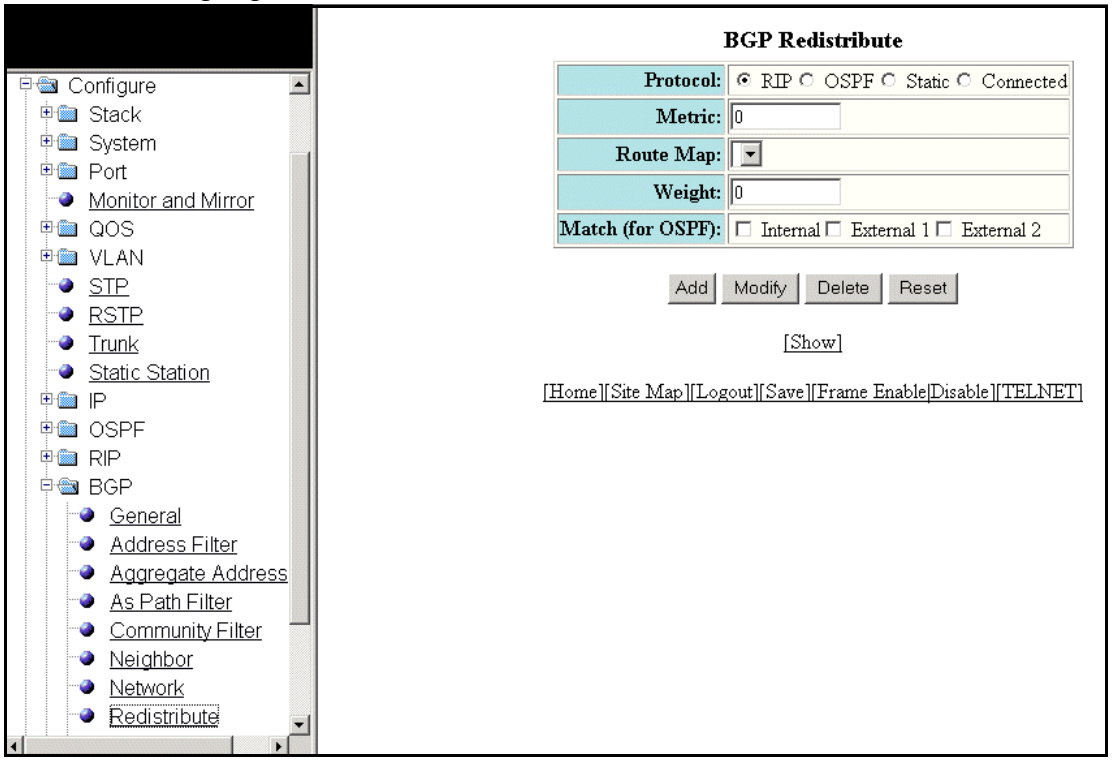
Configuring BGP redistribute parameters

To configure a BGP redistribute, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Redistribute**.

The **BGP Redistribute** window is displayed as shown in Figure 196.

FIGURE 196 Configuring a BGP redistribute



3. Click one of the following options for **Protocol**.
   - **RIP** - Redistributes RIP routes into BGP.
   - **OSPF** - Redistributes OSPF routes into BGP
   - **Static** - Redistributes IP static routes into BGP.
   - **Connected** - Redistributes routes to a directly connected network into BGP.
4. Type the metric value from 0 through 4294967295 in the **Metric** field. The default value is zero.
5. Select the route map that is to be consulted before adding the RIP route to the BGP route table in the **Route Map** list.
6. Type the weight for the route in the **Weight** field.
7. Select one of the following types of OSPF routes to be redistributed into BGP for **Mode (for OSPF)**:
   - **Internal**
   - **External 1**
   - **External 2**

   NOTE
   Step 7 applies only to the OSPF protocol.
8. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP redistribute, click **Show**.

To modify the configured BGP redistribute, click **Modify**. You can also delete the BGP redistribute by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

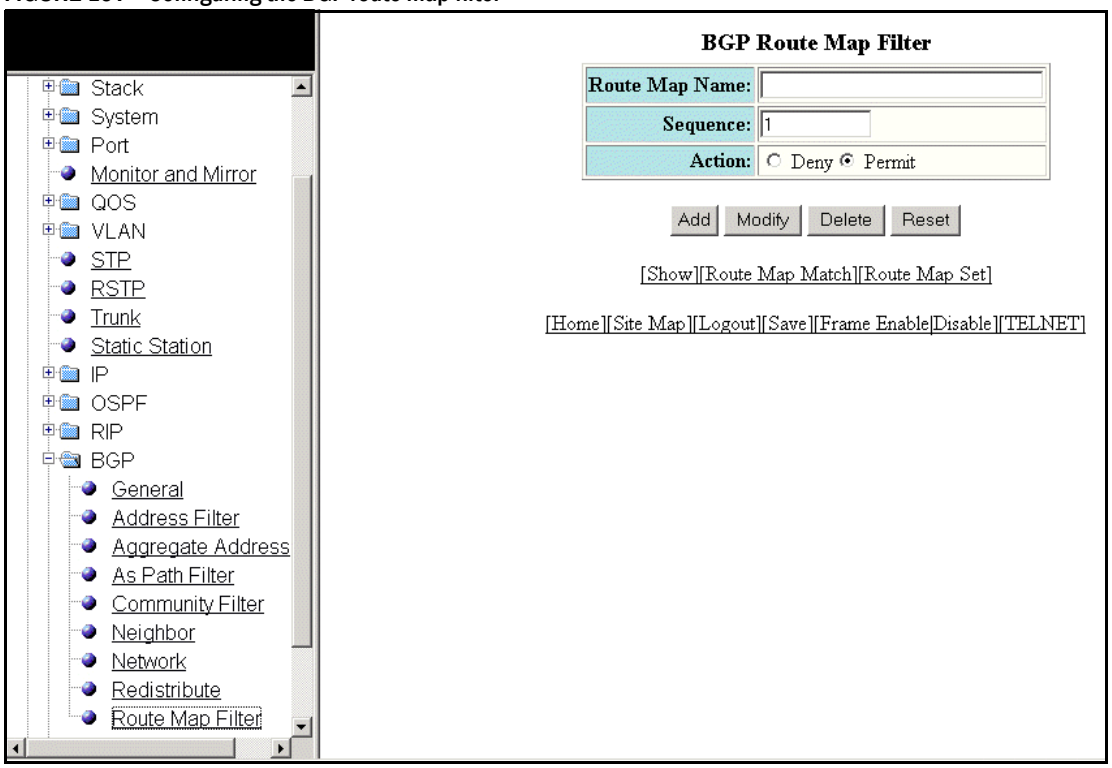
Configuring a BGP route map filter

To configure a BGP route map filter, perform the following steps.

1. Click **Configure** on the left pane and select **BGP**.
2. Click **Route Map Filter**.

The **BGP Route Map Filter** window is displayed as shown in Figure 197.

FIGURE 197 Configuring the BGP route map filter



3. Type a string of characters that names the route map in the **Route Map Name** field. Map names can be up to 32 characters in length.
4. Type an instance of the route map in the **Sequence** field. Each route map can have up to 50 instances.
5. Click **Deny** for **Action** to restrict the Layer 3 switch from advertising or learning the routes.

   Or

   Click **Permit** for **Action** so that the Layer 3 switch applies the match and sets statements associated with this route map instance.
6. Click **Add**.

The message **The change has been made** is displayed. To display the configured BGP route map filter, click **Show**.

To modify the configured BGP route map filter, click **Modify**. You can also delete the BGP route map filter by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **BGP Route Map Filter** window contains the following links:

- To configure a route map match statement, click **Route Map Match**. For more information, refer to "Configuring a route map match" on page 288.
- To configure a route map set, click **Route Map Set.** For more information, refer to "Configuring a route map set" on page 289.

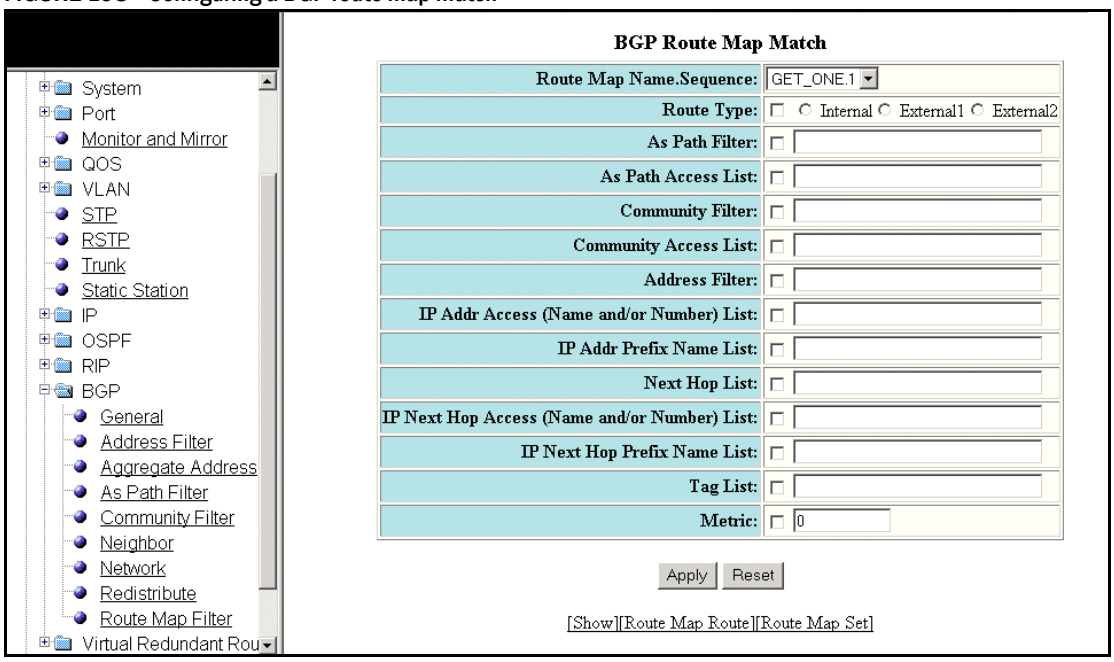
Configuring a route map match

To configure a route map match statement, perform the following steps.

1. Click **Route Map Match** on the **BGP Route Map Filter** window.

The **BGP Route Map Match** window is displayed as shown in Figure 198.

FIGURE 198 Configuring a BGP route map match



2. Select a router map name or sequence in the **Route Map Name.Sequence** list.
3. Select the **Route Type** check box and then click **Internal** or **External1** or **External2**.
4. Select the **As Path Filter** check box and then type the sequence of AS-path filters in the field.
5. Select the **As Path Access List** check box and then type the AS-path ACL in the field.
6. Select the **Community Filter** check box and then type the sequence of community filters in the field.
7. Select the **Community Access List** check box and then type the community ACL in the field.
8. Select the **Address Filter** check box and then type the sequence of address filters in the field.
9. Select the **IP Addr Access (Name and/or Number) List** check box and then type the IP address access name or number in the field.
10. Select the **IP Addr Prefix Name List** check box and then type an IP prefix list in the field.
11. Select the **Next Hop List** check box and then type the IP address of the next hop Layer 3 switch in the field.
12. Select the **IP Next Hop Access (Name and/or Number) List** check box and then type the IP next hop access name or number in the field.
13. Select the **IP Next Hop Prefix Name List** check box and then type the IP next hop prefix list in the field.

14. Select the **Tag List** check box and then type the route tag in the field.
15. Select the **Metric** check box and then type the route BGP MED in the field.
16. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

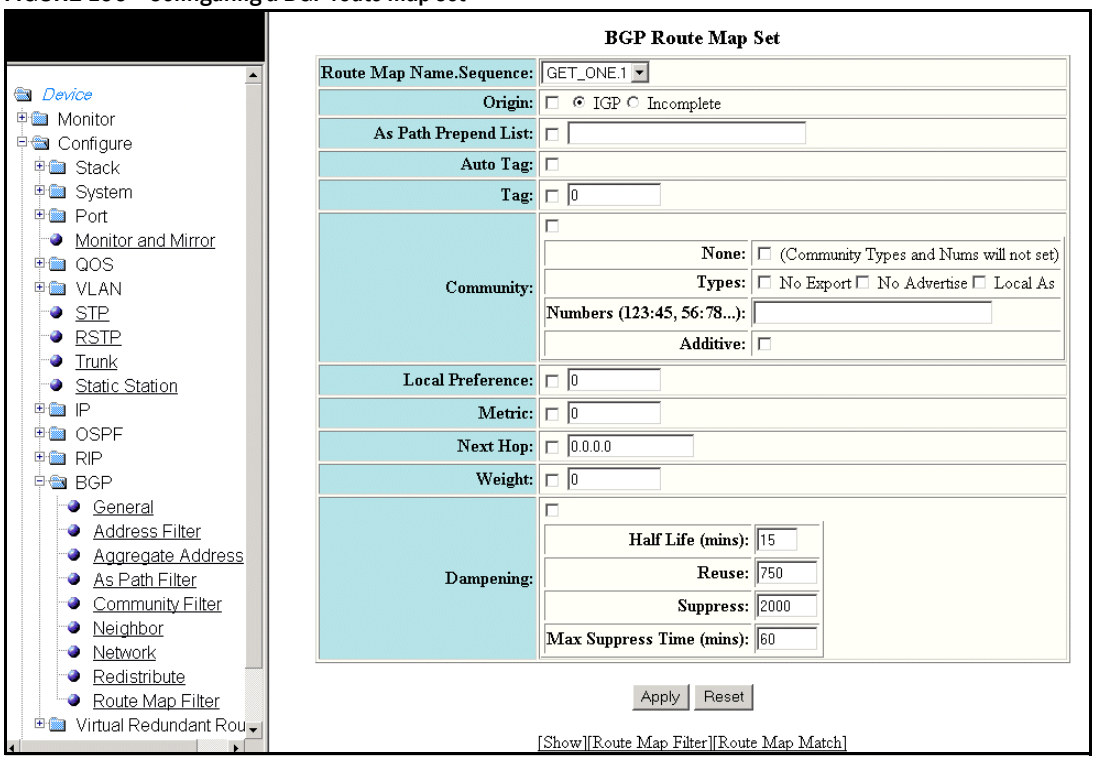
Configuring a route map set

To configure a route map set, perform the following steps.

1. Click **Route Map Set** on the **BGP Route Map Filter** window.

The **BGP Route Map Set** window is displayed as shown in Figure 199.

FIGURE 199 Configuring a BGP route map set



2. Select a router map name or sequence in the **Route Map Name.Sequence** list.
3. Select the **Origin** check box and then click **IGP** or **Incomplete**.
4. Select the **As Path Prepend List** check box and then type AS numbers that can be prefixed to the route AS-path.
5. Select the **Auto Tag** check box to add an automatically calculated tag to the route.
6. Select the **Tag** check box and then type the tag to the route in the field.

7. Select the **Community** check box and then do one the following:
    - **None** - Select the **None** check box so that the community types and numbers will not be set.
    - **Types** - Select the **Types** check box and then select **No Export** or **No Advertise** or **Local As**.
    - **Numbers** - Type a community value in *num*:*num* format in the field.
    - **Additive** - Select the **Additive** check box.
8. Select the **Local Preference** check box and then type the local preference in the field.
9. Select the **Metric** check box and then type the MED value in the field.
10. Select the **Next Hop** check box and then type the IP address of the next hop router in the field.
11. Select the **Weight** check box and then type the weight in the field.
12. Select the **Dampening** check box and then type the following formation:
    - **Half Life (mins)** - Type the half life time in minutes.
    - **Reuse** - Type the reuse threshold value.
    - **Suppress** - Type the suppression threshold value.
    - **Max Suppress Time (mins)** - Type the maximum suppression time in minutes.
13. Click **Apply**.

The message **The change has been made** is displayed. To reset the data entered in the configuration pane, click **Reset**.

Chapter

Configuring a Virtual Redundant Router 31

In this chapter

- Modifying a VRRP interface 291
- Configuring a VRRP virtual router 292
- Modifying a VRRP-E interface 296
- Configuring a VRRP-E virtual router 296
- Modifying a VSRP interface 299
- Configuring a VSRP virtual switch 301

NOTE
The Virtual Redundant Router feature is specific to Brocade FCX-ADV, Brocade ICX 6610, and Brocade FSX devices running Layer 3 code. In Brocade FSX devices, the Virtual Redundant Router feature is supported in the base Layer 3 software image also.

NOTE
The terms “Layer 3 switch” and “router” are used interchangeably in this chapter.

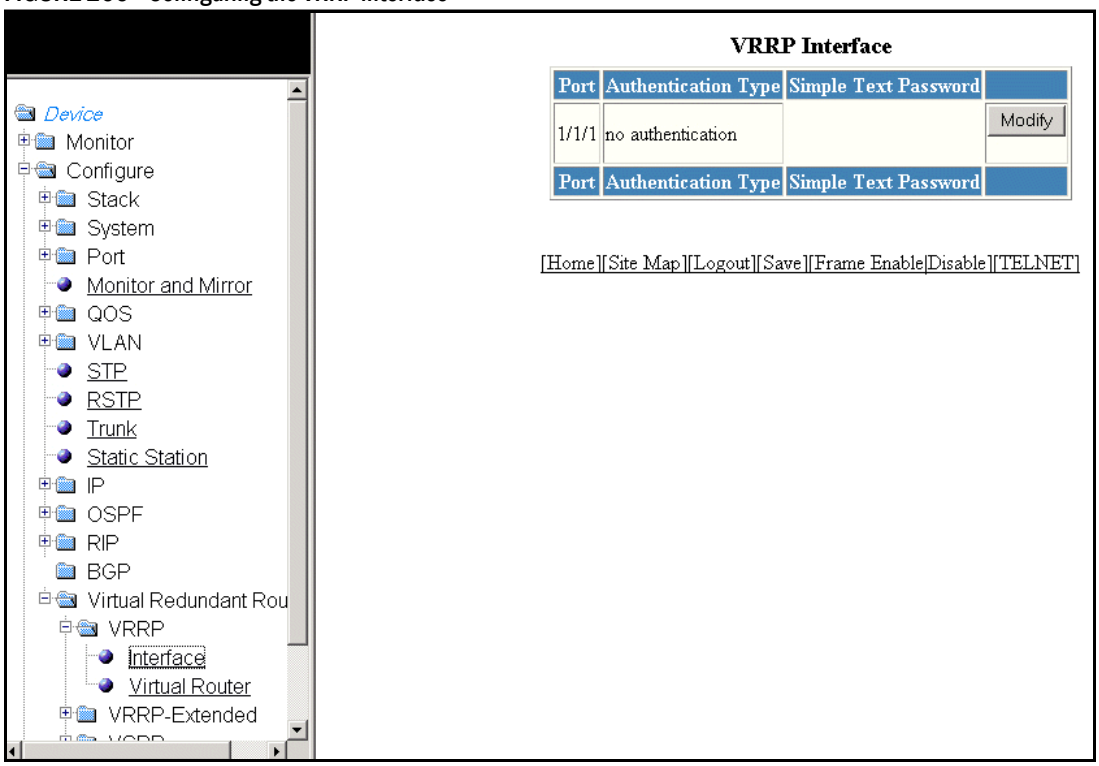
Modifying a VRRP interface

To modify a Virtual Router Redundancy Protocol (VRRP) interface, perform the following steps.

1. Click **Configure** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP** and then select **Interface**.

The **VRRP Interface** window is displayed as shown in Figure 200.

FIGURE 200 Configuring the VRRP interface



3. Click **Modify**.

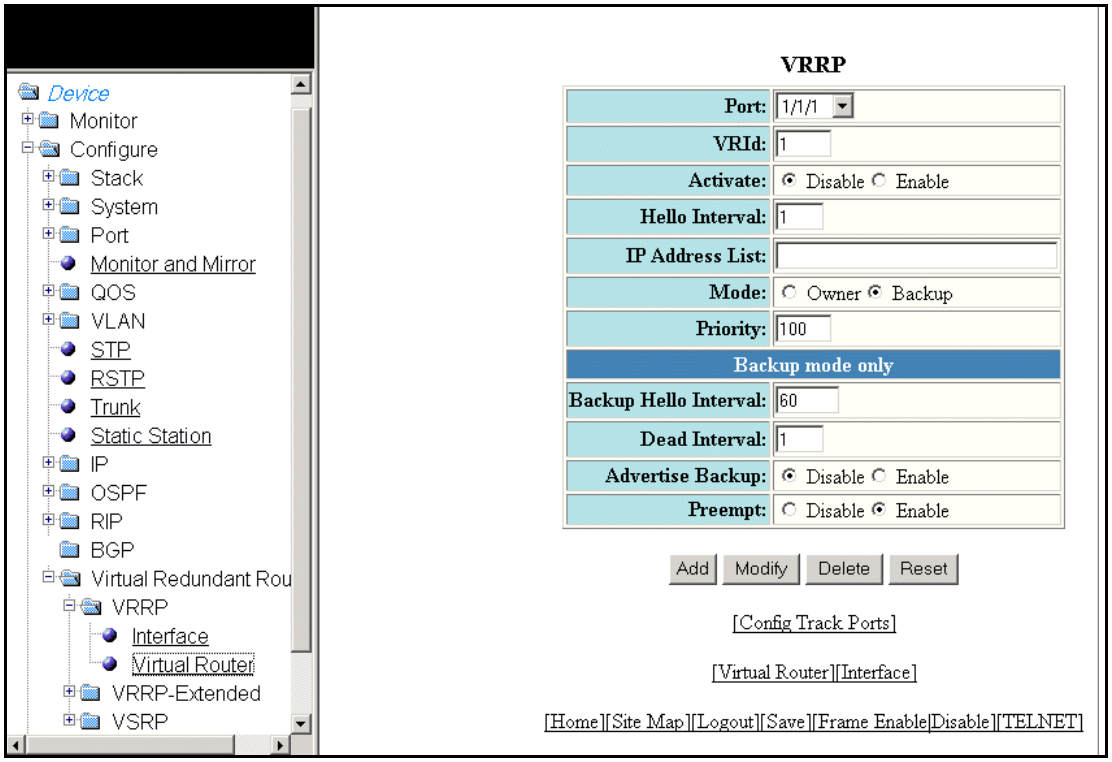
Configuring a VRRP virtual router

To configure a VRRP virtual router, perform the following steps.

1. Click **Configure** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP** and then select **Virtual Router**.

The **VRRP** window is displayed as shown in Figure 201.

FIGURE 201 Configuring a VRRP virtual router



3. Select an Ethernet port or virtual interface in the **Port** list.

   The Ethernet port number varies based on the product:

   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum

4. Type the Virtual Router Identifier (VRID) in the **VRId** field.
5. Click **Disable** or **Enable** for **Activate**.
6. Specify the hello interval from 1 through 84 seconds in the **Hello Interval** field. The default is one second.

   NOTE
   The default dead interval is three times the hello interval plus skew time, where skew time is equal to (256 - priority)/256. Generally, if you change the hello interval, you also must change the dead interval on the backup Layer 3 switches.

7. Type the IP address of the device in the **IP Address List** field.

   VRRP does not use virtual IP addresses. Instead, you must associate the virtual router with one or more real interface IP addresses configured on the Layer 3 switch that owns the real IP addresses.

8. Click **Owner** or **Backup** for **Mode**.
9. Type the VRRP priority that can be assigned for this interface and VRID in the **Priority** field. You can specify a value from 3 through 254. The default is 100.

10. Enter the following information for **Backup mode only**:
    - **Backup Hello Interval** - Type how often backup sends hello messages to the master. You can specify the interval from 60 through 3600 seconds. The default is 60 seconds.
    - **Dead Interval** - Type the number of seconds a backup must wait for a hello message from the master before determining that the master is dead. The dead interval can be configured from 1 through 84 seconds.
    - **Advertise Backup** - Click **Disable** or **Enable**. By default, advertise backup is disabled and the backup does not send hello messages to advertise themselves to the master.
    - **Preempt** - Click **Disable** or **Enable**. By default, preempt is enabled.
11. Click **Add**.

The message **The change has been made** is displayed. To modify the configured virtual router, click **Modify**. You can also delete the virtual router by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **VRRP** window contains the following links to configure VRRP parameters:

- To configure the track ports, click **Config Track Ports.** For more information, refer to "Configuring track ports" on page 294.
- To configure a VRRP router, click **Virtual Router**.
- To modify a VRRP interface, click **Interface**. For more information, refer to "Modifying a VRRP interface" on page 291.

Configuring track ports

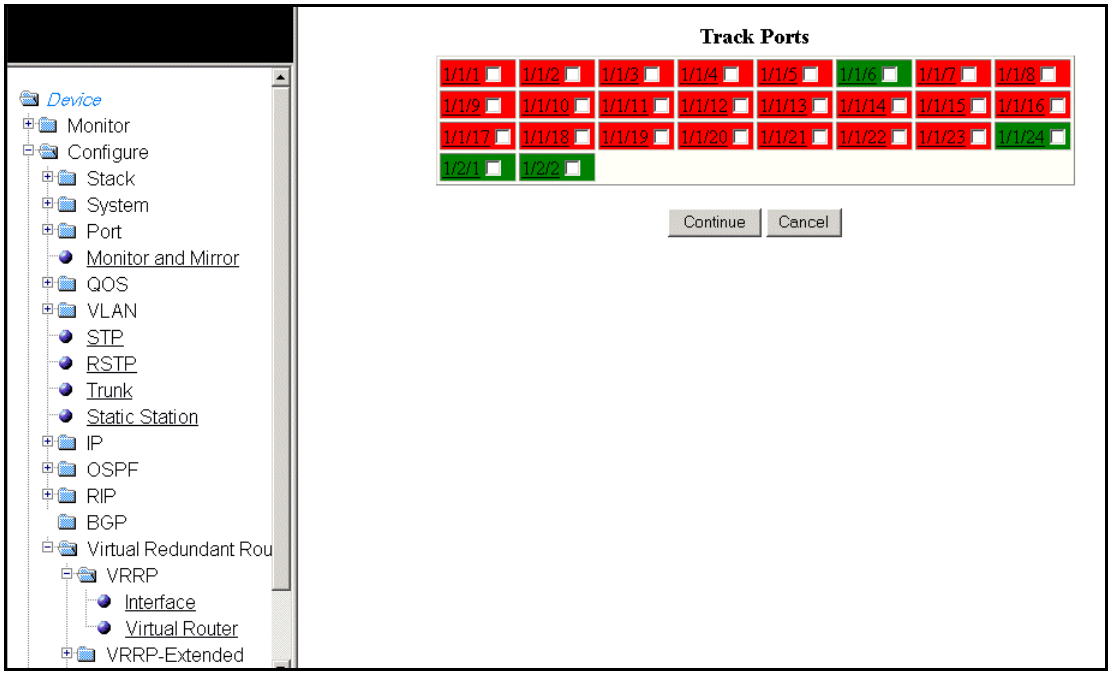
You can configure the VRID on one interface to track the link-state of another interface on the Layer 3 switch. This capability is useful for tracking the state of the exit interface for the path for which the VRID is providing redundancy.

To configure track ports, perform the following steps.

1. Click **Config Track Ports** on the **VRRP** window.

The **Track Ports** window is displayed as shown in Figure 202.

FIGURE 202 Configuring track ports



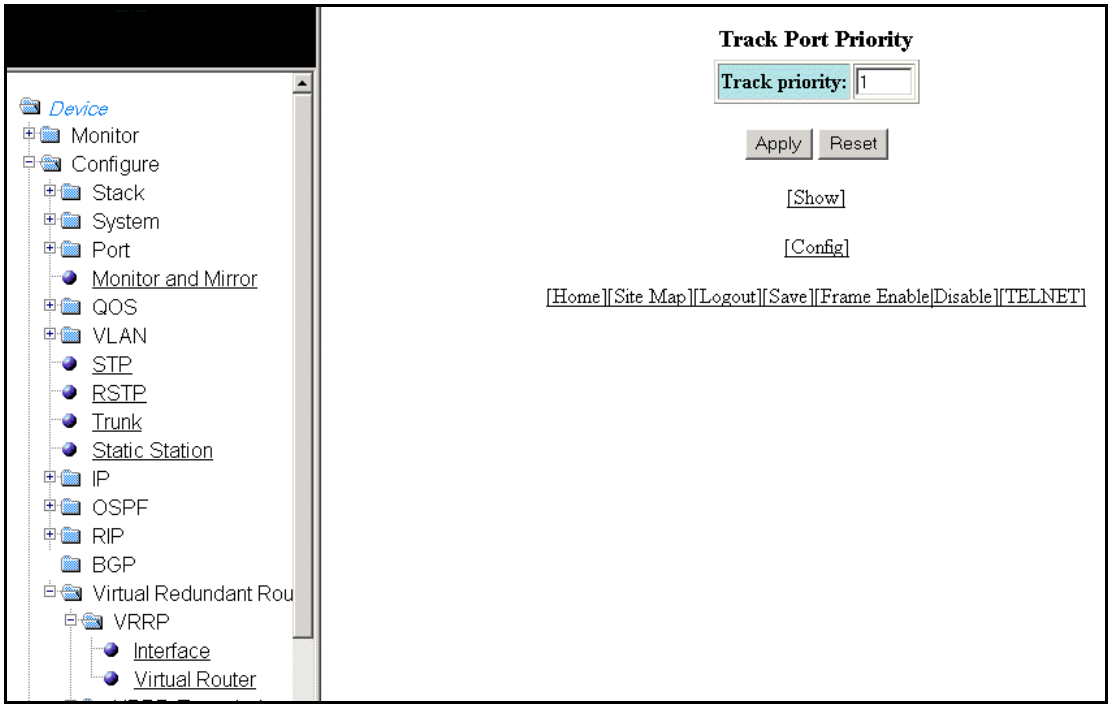
2. Select the ports.

   You can click on any port to display the real-time information for that port.

3. Click **Continue**.

The **Track Port Priority** window is displayed as shown in Figure 203.

FIGURE 203 Configuring track port priority



4. Type the priority of the track ports in the **Track priority** field. The default track priority for a VRRP owner is two and for backups it is one.

   When you configure a VRID to track the link-state of other interfaces, if one of the tracked interfaces goes down, the software changes the VRRP priority of the VRID interface to the track priority, which typically is lower than the VRID priority and lower than the VRID priorities configured on the backups.

5. Click **Apply**.

The message **The change has been made** is displayed. To display the configured VRRP virtual router, click **Show**.

Modifying a VRRP-E interface

The procedure to modify the Virtual Router Redundancy Protocol Extended (VRRP-E) interface is the same as the procedure to modify a VRRP interface. For more information on how to modify a VRRP-E interface, refer to "Modifying a VRRP interface" on page 291.

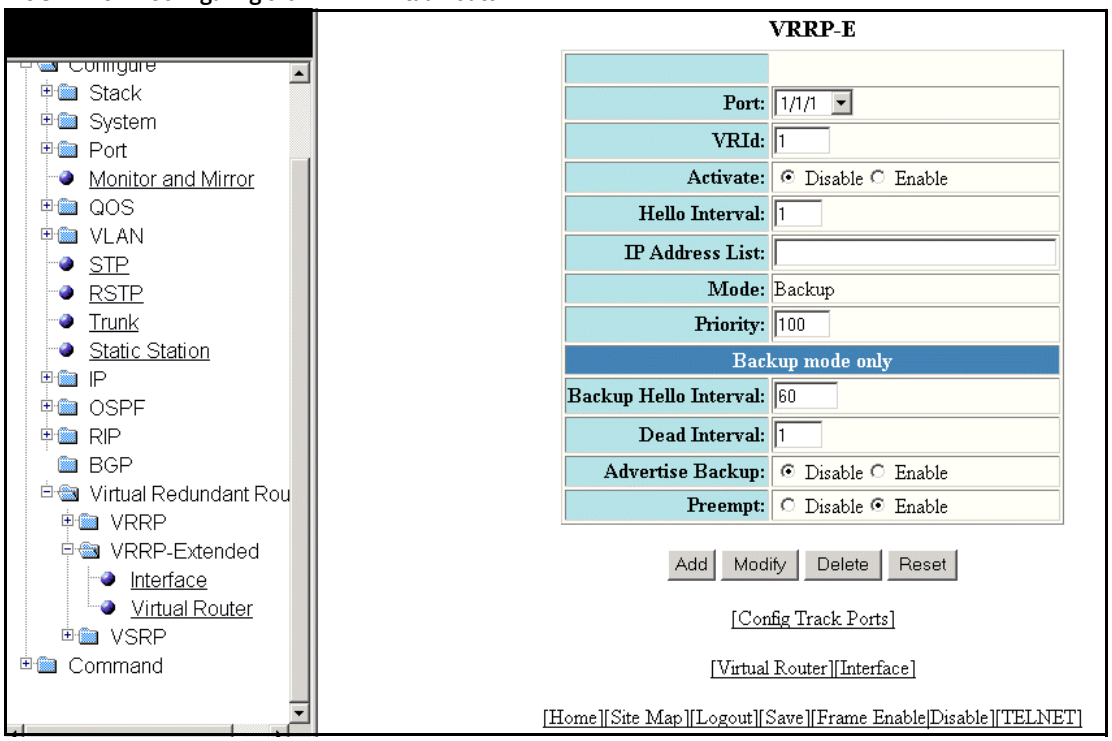
Configuring a VRRP-E virtual router

To configure a VRRP-E virtual router, perform the following steps.

1. Click **Configure** on the left pane and select **Virtual Redundant Router**.
2. Click **VRRP-Extended** and then select **Virtual Router**.

The **VRRP-E** window is displayed as shown in Figure 204.

FIGURE 204 Configuring the VRRP-E virtual router



3. Select an Ethernet port or virtual interface in the **Port** list.

   The Ethernet port number varies based on the product:

   - For Brocade FCX and Brocade ICX 6610 devices – stack-unit/slotnum/portnum
   - For Brocade FSX devices – slotnum/portnum

4. Type the virtual router identifier in the **VRId** field.
5. Click **Disable** or **Enable** for **Activate**.
6. Type the hello interval from 1 through 84 seconds in the **Hello Interval** field. The default is one second.

   NOTE
   The default dead interval is three times the hello interval plus skew time, where skew time is equal to (256 - priority)/256. Generally, if you change the hello interval, you also should change the dead interval on the backup Layer 3 switches.

7. Type the virtual router IP address in the **IP Address List** field.

   The virtual router IP address must be in the same subnet as a real IP address configured on the VRRP-E interface, but cannot be the same as a real IP address configured on the interface.

8. Type the VRRP-E priority that can be assigned for this interface and VRID in the **Priority** field. You can specify a value from 3 through 254. The default is 100.
9. Enter the following information for **Backup mode only**:

   - **Backup Hello Interval** - Type how often backup sends hello messages to the master. You can specify the interval from 60 through 3600 seconds. The default is 60 seconds.
   - **Dead Interval** - Type the number of seconds a backup should wait for a hello message from the master before determining that the master is dead. The dead interval can be configured from 1 through 84 seconds.
   - **Advertise Backup** - Click **Disable** or **Enable**. By default, advertise backup is disabled and the backup does not send hello messages to advertise themselves to the master.
   - **Preempt** - Click **Disable** or **Enable**. By default, preempt is enabled.

10. Click **Add**.

The message **The change has been made** is displayed. To modify the configured virtual router, click **Modify**. You can also delete the virtual router by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

The **VRRP** window provides the following links to configure VRRP-E parameters:

- To configure track ports, click **Config Track Ports.** For more information, refer to "Configuring track ports" on page 298.
- To configure a VRRP router, click **Virtual Router**.
- To modify a VRRP-E interface, click **Interface**. For more information, refer to "Modifying a VRRP-E interface" on page 296.

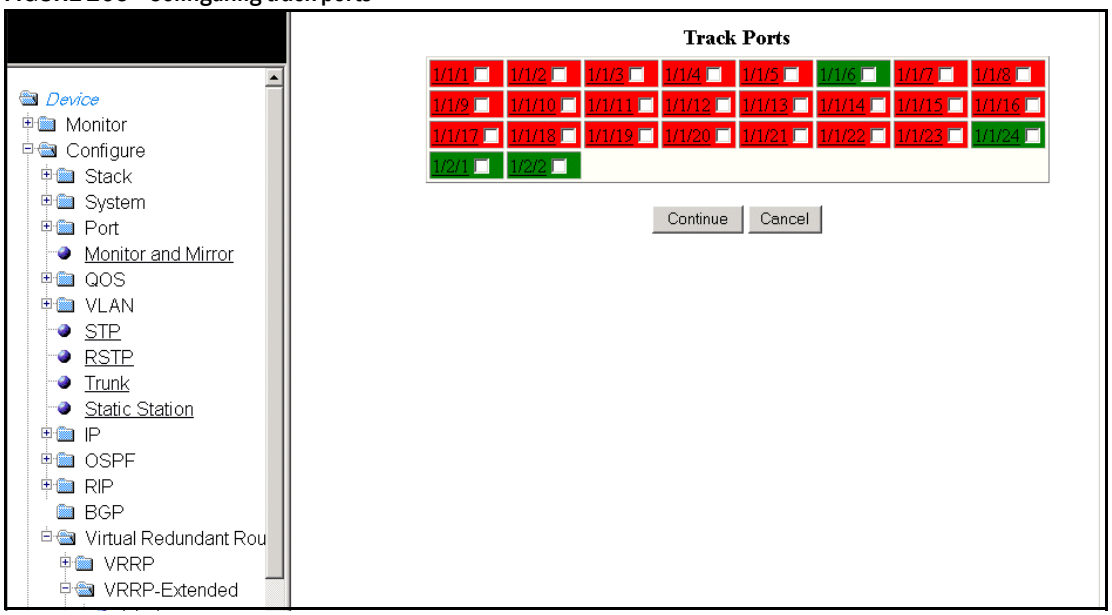
Configuring track ports

To configure track ports, perform the following steps.

1. Click **Config Track Ports** on the **VRRP-E** window.

The **Track Ports** window is displayed as shown in Figure 205.

FIGURE 205 Configuring track ports



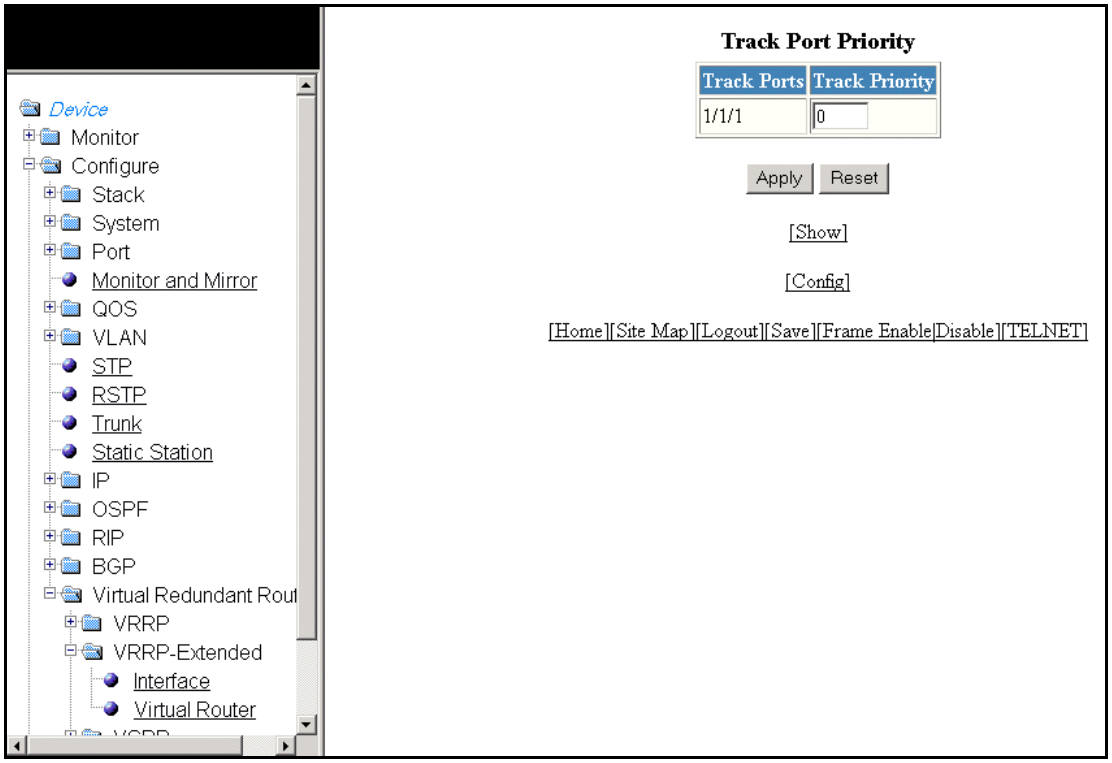
2. Select the ports.

   You can click on any port to open the real-time information for that port.

3. Click **Continue**.

The **Track Port Priority** window is displayed as shown in Figure 206.

FIGURE 206 Configuring track port priority



4. Type the priority of the track ports in the **Track priority** field.

   When you configure a VRID to track the link-state of other interfaces, if one of the tracked interfaces goes down, the software reduces the VRRP-E priority of the VRID by the amount of the priority of the tracked interface that went down.

5. Click **Apply**.

The message **The change has been made** is displayed. Click **Show** to display the configured VRRP-E virtual router.

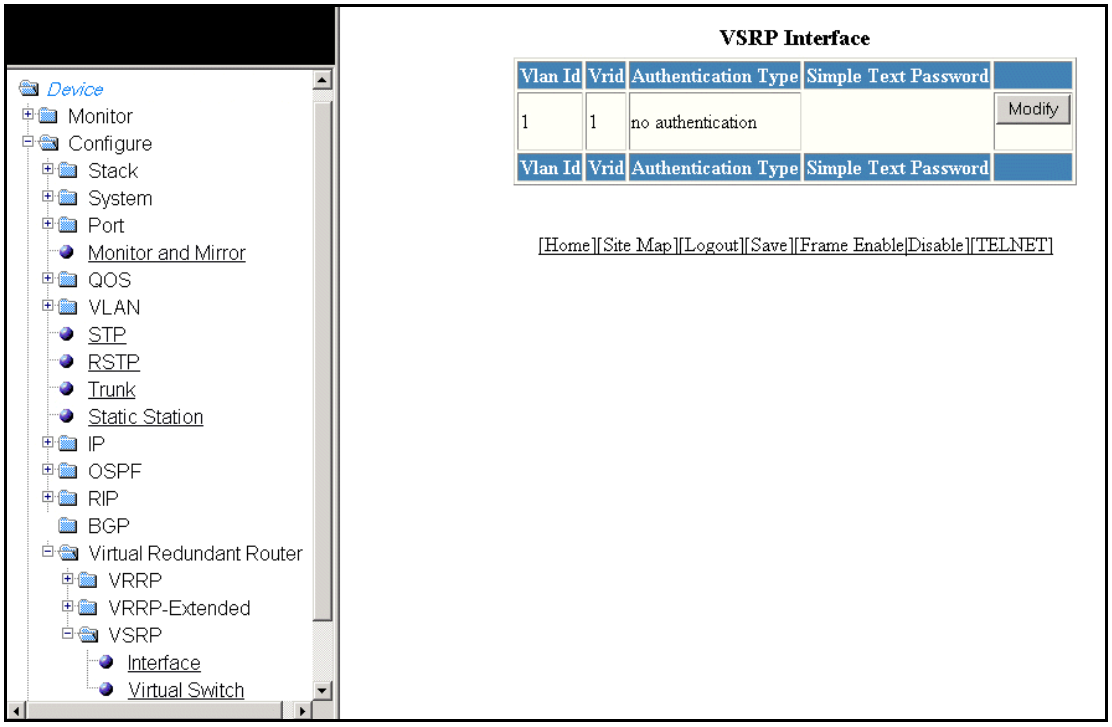
Modifying a VSRP interface

To modify a Virtual Switch Redundancy Protocol (VSRP) switch, perform the following steps.

1. Click **Configure** on the left pane and select **Virtual Redundant Router**.
2. Click **VSRP** and then select **Interface**.

The **VSRP Interface** window is displayed as shown in Figure 207.

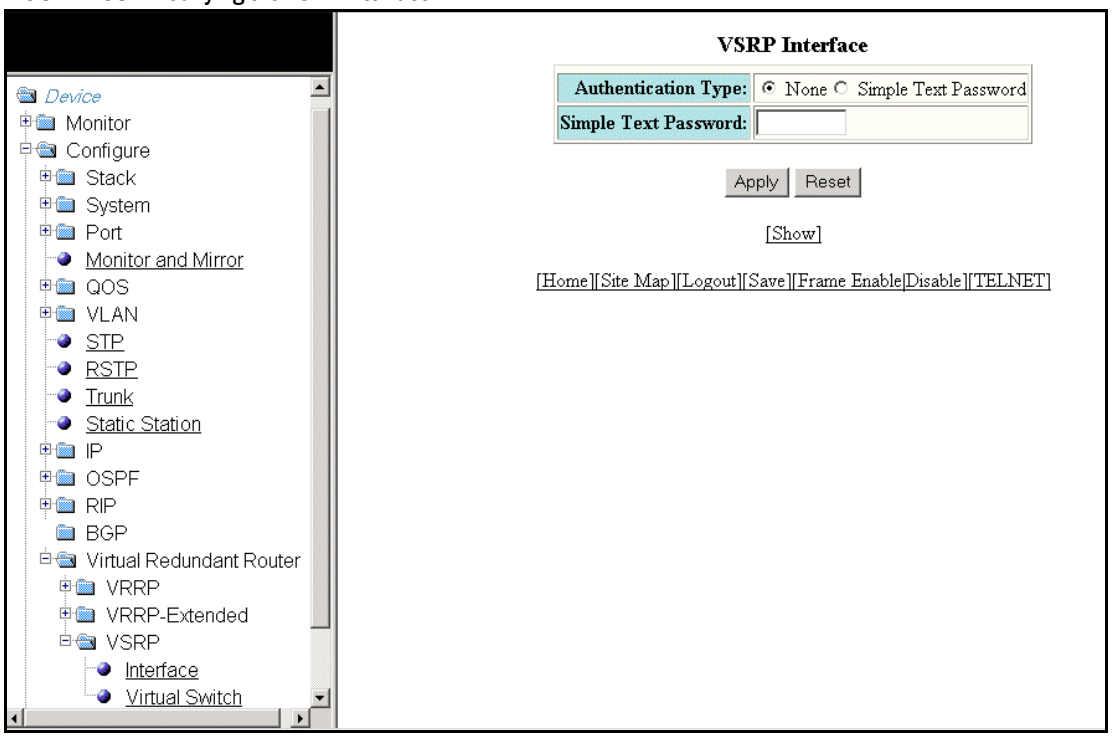
FIGURE 207 Configuring the VSRP Interface



3. Click **Modify**.

The **VSRP Interface** window is displayed shown in Figure 208.

FIGURE 208 Modifying the VSRP interface



4. Select one of the following for **Authentication Type**:
   - **None** - The interfaces do not use authentication. This is the default.
   - **Simple Text Password** - The interfaces use a simple text string as a password in packets sent on the interface.
5. Type a character string in the **Simple Text Password** field.
6. Click **Apply**.

The message **The change has been made** is displayed. Click **Show** to display the VSRP interface. To reset the data entered in the configuration pane, click **Reset**.

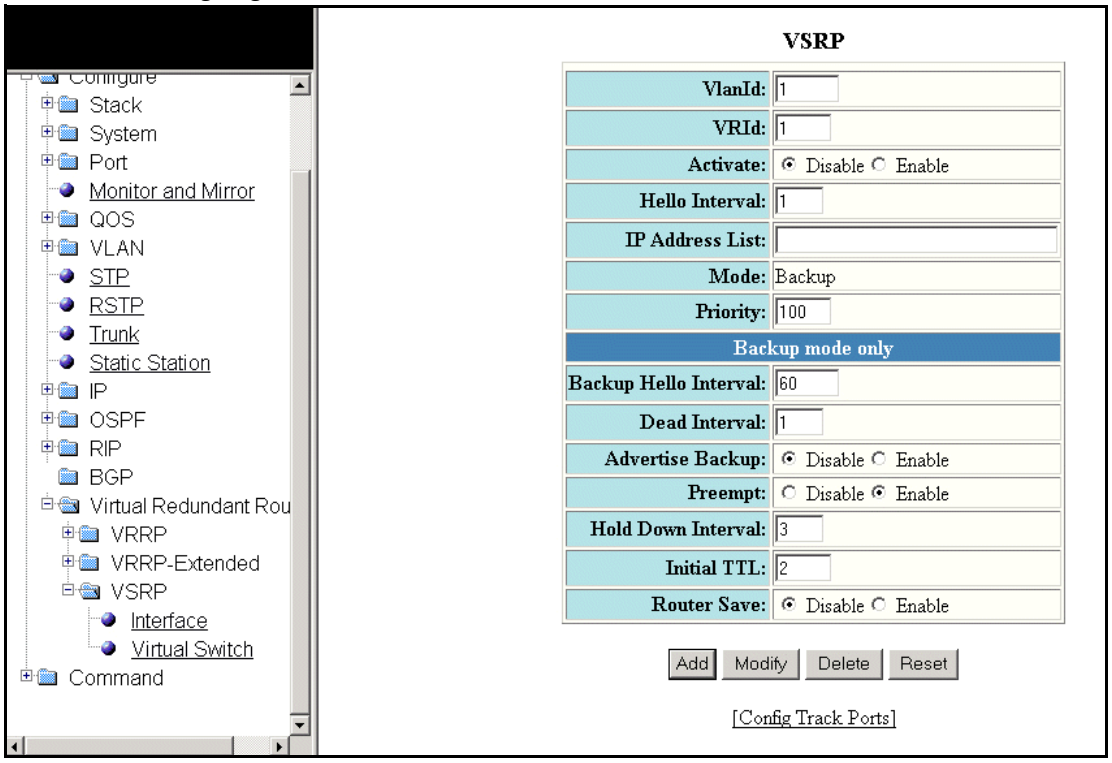
Configuring a VSRP virtual switch

To configure a VSRP switch, perform the following steps.

1. Click **Configure** on the left pane and select **Virtual Redundant Router**.
2. Click **VSRP** and then select **Virtual Switch**.

The **VSRP** window is displayed as shown in Figure 209.

FIGURE 209 Configuring the VSRP switch



3. Type the port-based VLAN identifier in the **VlanId** field.
4. Type the identifier of the virtual switch in the **VRId** field.
5. Click **Disable** or **Enable** for **Activate**.

6. Type the hello interval from 1 through 84 seconds in the **Hello Interval** field. The default is one second.
7. Type the IP address of the device in the **IP Address List** field.
8. Type the backup priority in the **Priority** field.
9. Enter the following information for **Backup mode only**:
    - **Backup Hello Interval** - Type the backup hello interval; that is, how often the backup sends a hello message to the master. The range is from 60 through 3600 seconds. The default is 60 seconds.
    - **Dead Interval** - Type the number of seconds a backup should wait for a hello message from the master before determining that the master is dead. The default is 3 seconds. This is three times the default hello interval.
    - **Advertise Backup** - Click **Disable** or **Enable**. By default, the advertise backup is disabled and the backups do not send hello messages to advertise themselves to the master.
    - **Preempt** - Click **Disable** or **Enable**.
    - **Hold Down Interval** - Type the hold down interval, which prevents Layer 2 loops from occurring during failover, by delaying the new master from forwarding traffic long enough to make sure that the failed master is unavailable. The range is from 1 through 84 seconds. The default is two seconds.
    - **Initial TTL** - Type the number of hops the packet can traverse before being dropped. A hop can be a Layer 2 switch or a Layer 3 switch. The range is from 1 through 255 hops. The default is two hops.
    - **Router Save** - Click **Disable** or **Enable**.
10. Click **Add**.

The message **The change has been made** is displayed. To modify the configured virtual switch, click **Modify**. You can also delete the virtual switch by clicking **Delete**. To reset the data entered in the configuration pane, click **Reset**.

To configure track ports, click **Config Track Ports.** For more information, refer to "Configuring track ports" on page 302.

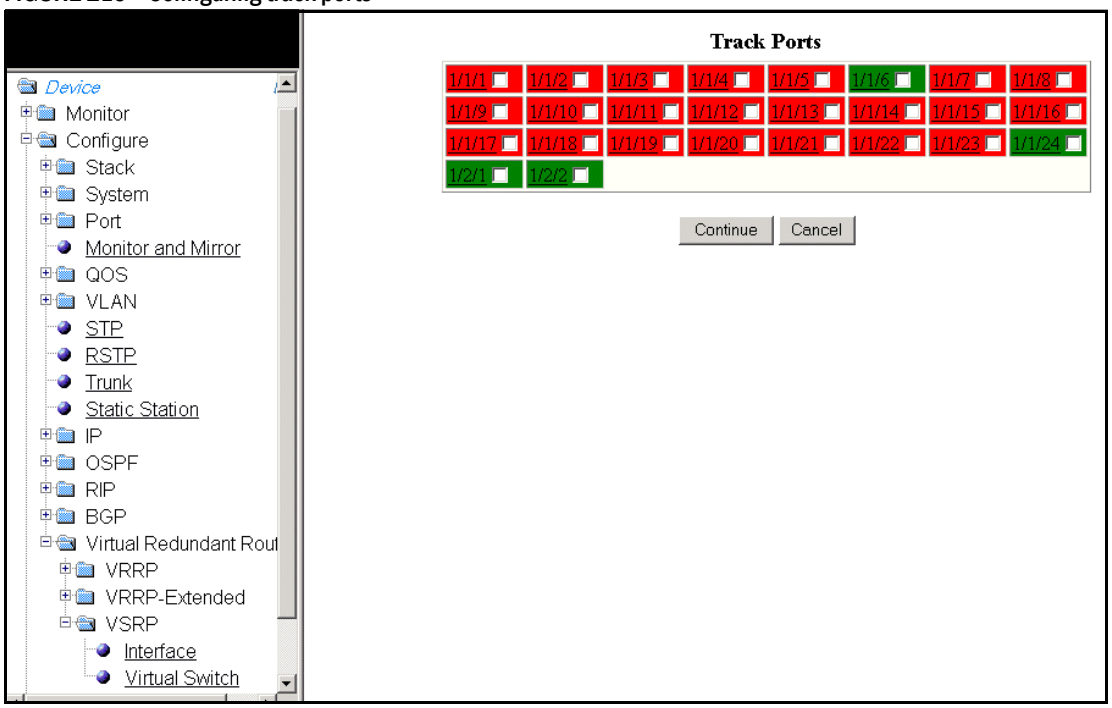
Configuring track ports

To configure track ports, perform the following steps.

1. Click **Config Track Ports** on the **VSRP** window.

The **Track Ports** window is displayed as shown in Figure 210.

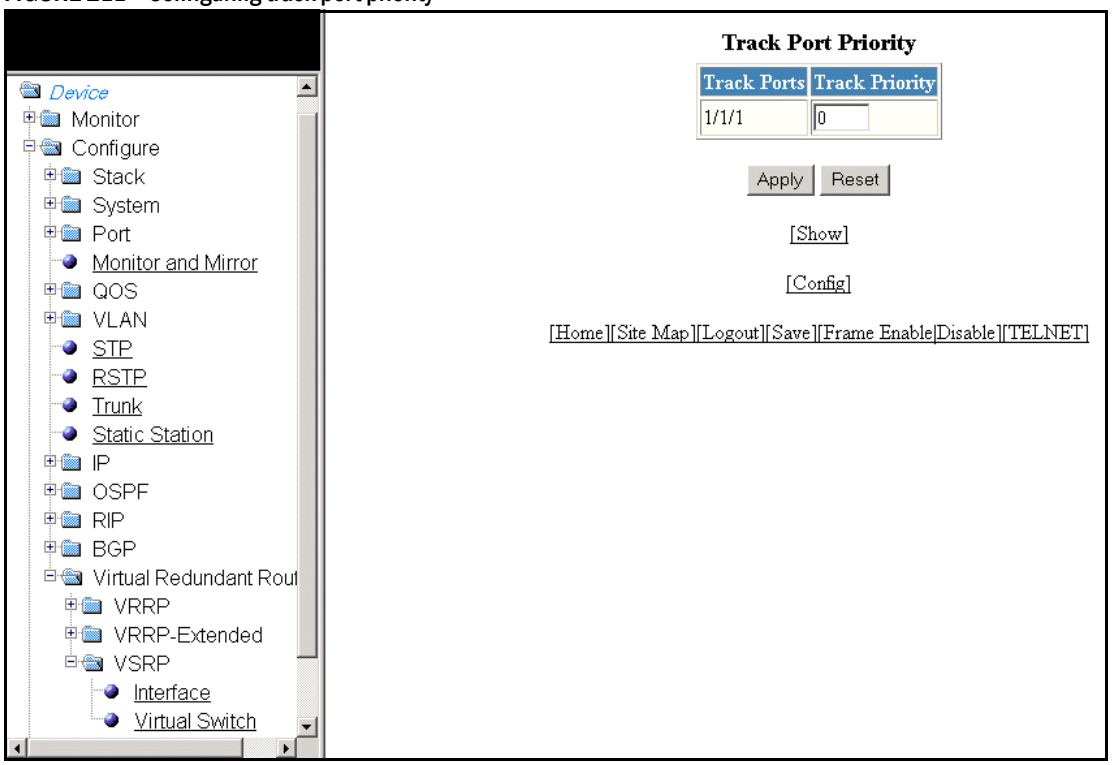
FIGURE 210 Configuring track ports



2. Select the ports. Click on any port to open the real-time information for that port.
3. Click **Continue**.

The **Track Port Priority** window is displayed as shown in Figure 211.

FIGURE 211 Configuring track port priority



4. Type the priority of the track ports in the **Track priority** field. The default track priority for all track ports is one.

   When you configure a VRID to track the link-state of other interfaces, if one of the tracked interfaces goes down, the software reduces the VSRP priority of the VRID by the amount of the priority of the tracked interface that went down.

5. Click **Apply**.

The message **The change has been made** is displayed. To display the configured VSRP virtual router, click **Show**.

Section

III

Device Commands

This section describes **Command** features, and includes the following chapters:

- Basic Device Commands 307
- Using TFTP 317

Chapter

32

Basic Device Commands

In this chapter

- Clearing information for a Layer 2 switch 307
- Clearing information for a Layer 3 switch 308
- Disabling or enabling the menu view 309
- Logging out 309
- Reloading units in a stack 310
- Saving the configuration to flash 311
- Switching over to the active role 311
- Performing hitless-reload from primary images 312
- Performing hitless-reload from secondary images 313
- Accessing the Telnet command prompt 314
- Performing a trace 315

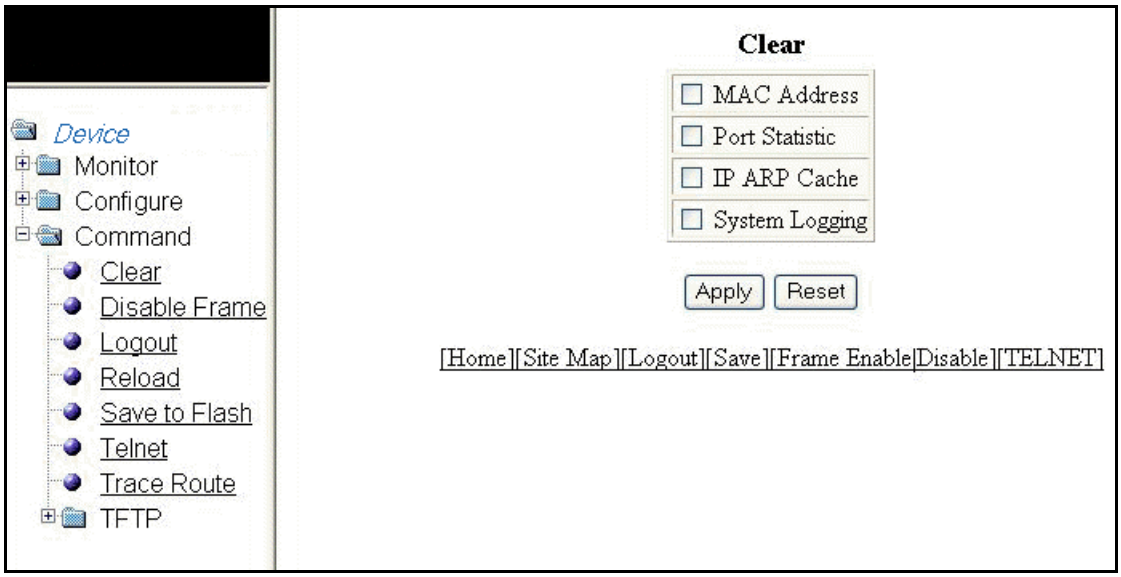
Clearing information for a Layer 2 switch

To clear specific data related to a Layer 2 switch, perform the following steps.

1. Click **Command** on the left pane and select **Clear.**

The **Clear** window is displayed as shown in Figure 212.

FIGURE 212 Clear window



2. Select the following check boxes to clear information:
   - **MAC Address**
   - **Port Statistic**
   - **IP ARP Cache**
   - **System Logging**
3. Click **Apply**.

All the current entries will be deleted.

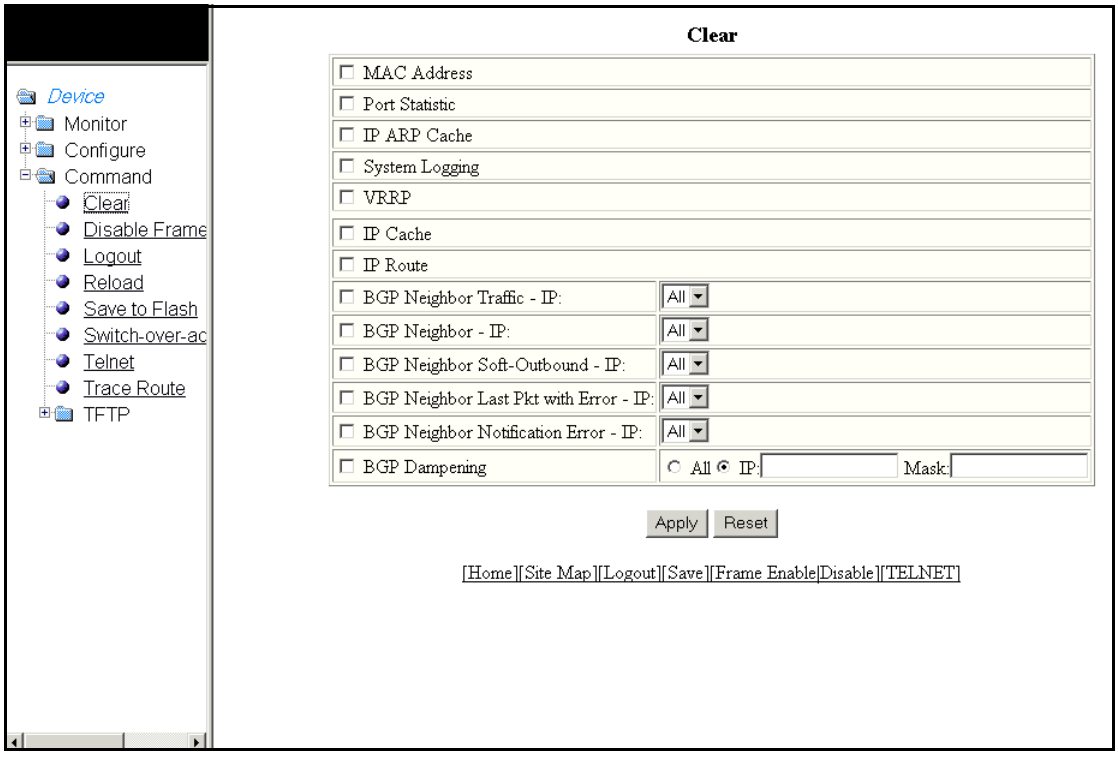
Clearing information for a Layer 3 switch

To clear specific data related to a Layer 3 switch, perform the following steps.

1. Click **Command** on the left pane and select **Clear.**

The **Clear** window is displayed as shown in Figure 213.

FIGURE 213 Clear window



2. Select the following check boxes to clear information:
   - **MAC Address**
   - **Port Statistic**
   - **IP ARP Cache**
   - **System Logging**
   - **VRRP**

- **IP Cache**
- **IP Route**
- **BGP Neighbor Traffic - IP** – Select **All** in the list to clear the BGP message counter for all neighbors.
- **BGP Neighbor - IP** – Select **All** in the list to close all neighbor sessions and clear all the routes exchanged by the Layer 3 switch and the neighbors.
- **BGP Neighbor Soft-Outbound - IP** – Select **All** in the list to update all outbound routes by applying the new or changed filters.
- **BGP Neighbor Last Pkt with Error - IP** – Select **All** in the list to clear the last packet from the neighbors that contained an error.
- **BGP Neighbor Notification Error - IP** – Select **All** in the list to clear the buffer for all neighbors containing the last NOTIFICATION message sent or received.
- **BGP Dampening** – Perform one of the following tasks:
  - Click **All** to clear all the route dampening statistics.
  - Click **IP** and type the network IP address in the **IP** field and the network mask in the **Mask** field.

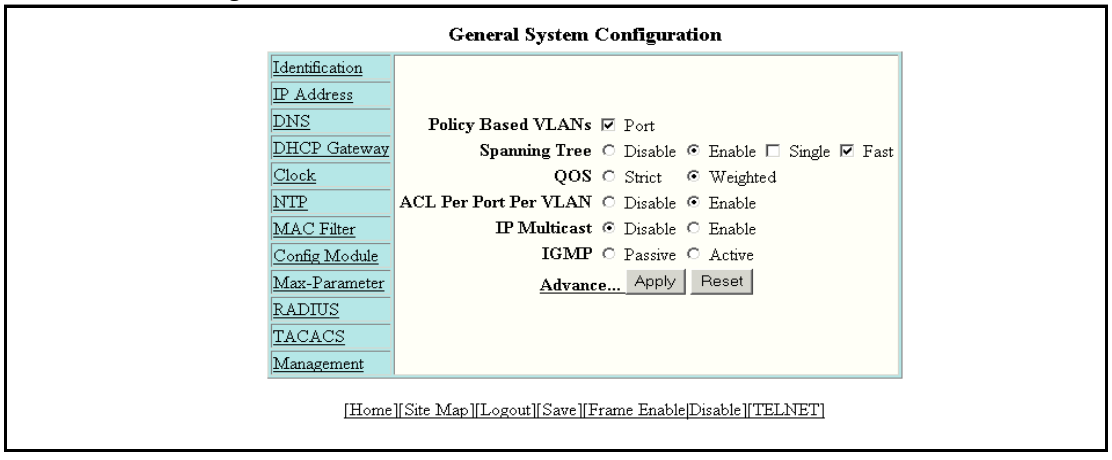
3. Click **Apply**.

All the current entries will be deleted.

Disabling or enabling the menu view

To enable or disable the menu view, click **Command** on the left pane and select **Disable Frame.** The menu tree from the left panel is hidden as shown in Figure 214. Click **Frame Enable** to view the menu tree.

FIGURE 214 Disabling the menu tree



Logging out

To exit the Web Management Interface, click **Command** on the left pane and select **Logout**. The login window is displayed as shown in Figure 215. To re-log in, click **Login** on the window.

FIGURE 215 Logging out

Reloading units in a stack

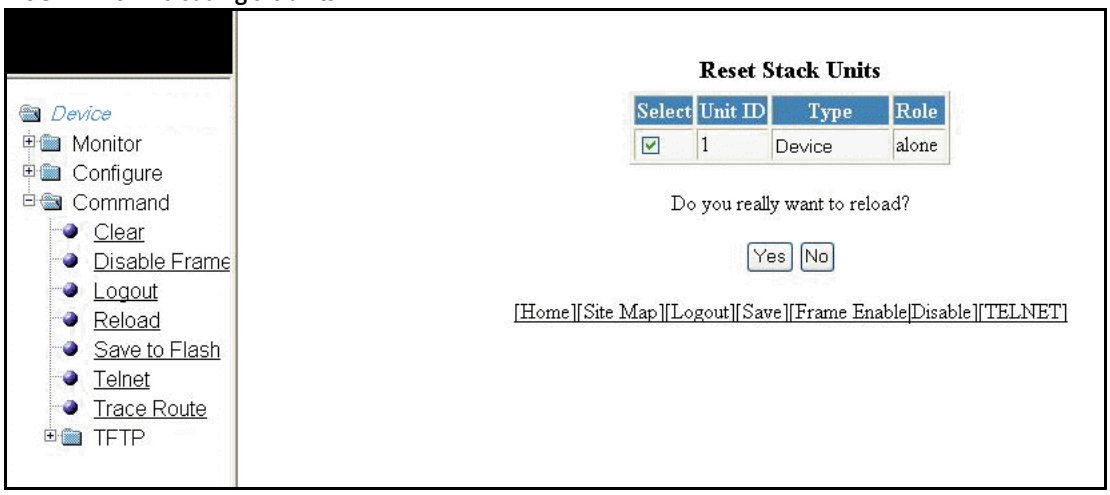
NOTE
This section is applicable to Brocade FCX-ADV and Brocade ICX 6610 devices.

To reload any or all of the units within a device, perform the following steps.

1. Click **Command** on the left pane and select **Reload**.

The **Reset stack units** window is displayed as shown in Figure 216.

FIGURE 216 Reloading the units



2. Click **Yes** to start the process.

NOTE
For Brocade FCX and Brocade ICX 6610 devices, if the Active Controller is reset or removed from the stack, the entire stack reloads and Active Controller and Standby Controller elections are started. If the unit functioning as the previous Active Controller is no longer part of the stack, the Standby Controller unit becomes the new Active Controller. After a reset, if no stack member qualifies as the Active Controller, the existing Standby Controller waits 30 seconds and then assumes the role of the Active Controller.

If both the Active Controller and the Standby Controllers are removed, the rest of the stack continues to function. The stack members will not be able to learn any new addresses.

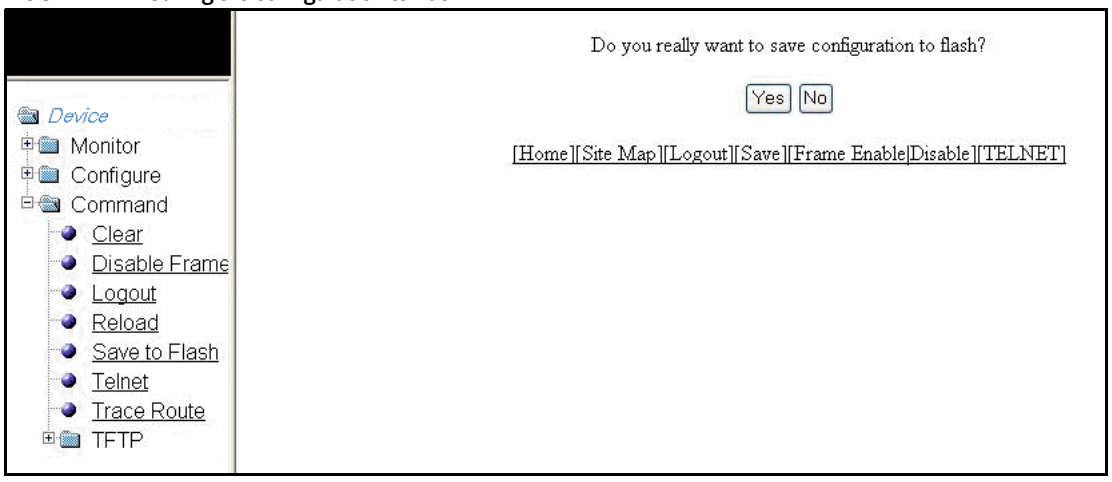
Saving the configuration to flash

To save the configuration changes to flash, perform the following tasks.

1. Click **Command** on the left pane and select **Save To Flash**.

The save configuration window is displayed as shown in Figure 217.

FIGURE 217 Saving the configuration to flash



2. Click **Yes** to confirm saving the configuration.

NOTE
To apply the changes to memory allocation, reload the software after you save the changes to the startup-configuration file.

Switching over to the active role

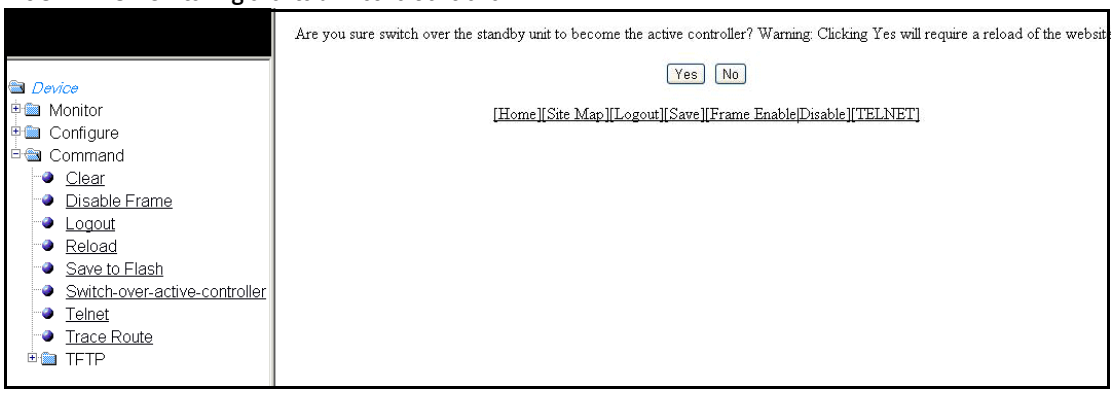
To switch a standby module to become an Active Controller, perform the following steps.

1. Click **Command** on the left pane and select **Switch-over-active-controller**.

NOTE
For Brocade FSX devices, select **Switch-over-active-role**.

The switch over window is displayed as shown in Figure 218.

FIGURE 218 Switching over to an Active Controller



2. Click **Yes** to switch the standby module to become an Active Controller or click **No** to cancel the operation.

Performing hitless-reload from primary images

NOTE
Hitless-reload is supported on Brocade FSX devices and applies to both Layer 2 and Layer 3 protocols. The Hitless-reload command is not supported on Brocade FCX and Brocade ICX 6610 devices.

To perform a hitless-reload of the system from a primary image, perform the following steps.

1. Click **Command** on the left pane and select **Hitless-reload**.
2. Click **Primary**.

The primary hitless-reload window is displayed as shown in Figure 219.

FIGURE 219 Hitless-reload from the primary image

3. Click **Yes** to reload the system from the primary image or click **No** to cancel the operation.

Performing hitless-reload from secondary images

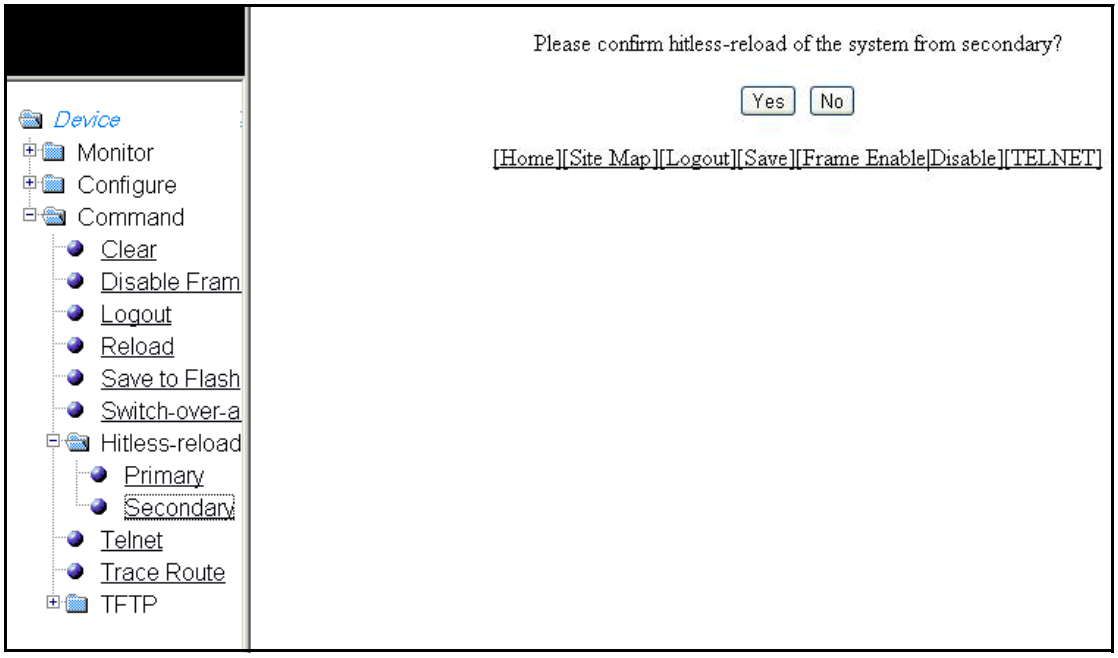
NOTE
Hitless-reload is supported on Brocade FSX devices and applies to both Layer 2 and Layer 3 protocols. The Hitless-reload command is not supported on Brocade FCX and Brocade ICX 6610 devices.

To perform a hitless-reload of the system from a secondary image, perform the following steps.

1. Click **Command** on the left pane and select **Hitless-reload**.
2. Click **Secondary**.

The secondary hitless-reload window is displayed as shown in Figure 220.

FIGURE 220 Hitless-reload from a secondary image



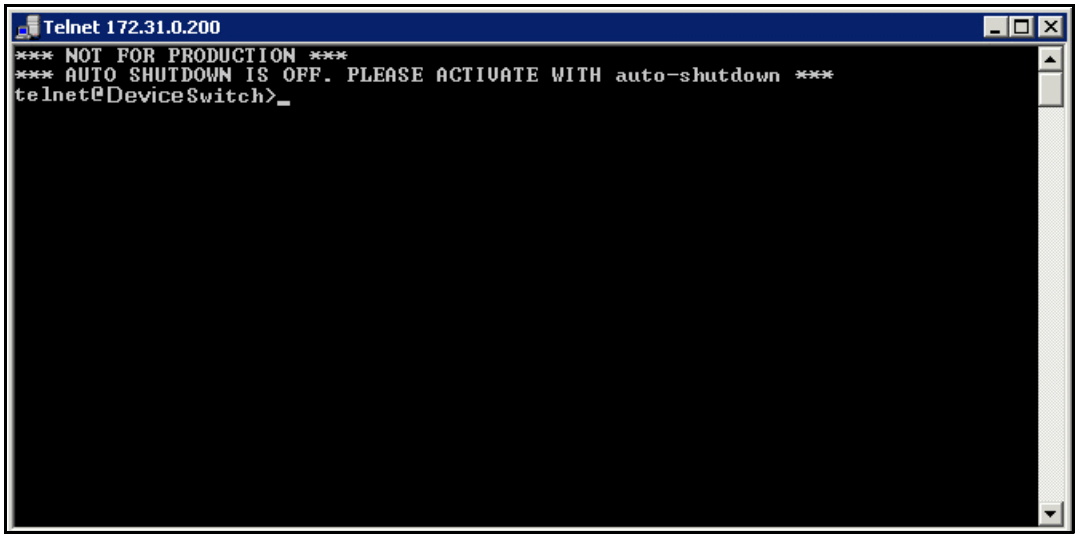
3. Click **Yes** to reload the system from the secondary image or click **No** to cancel the operation.

Accessing the Telnet command prompt

To open a Telnet CLI window, click **Command** on the left pane and select **Telnet**.

The **Telnet** window is displayed as shown in Figure 221.

FIGURE 221 Accessing Telnet



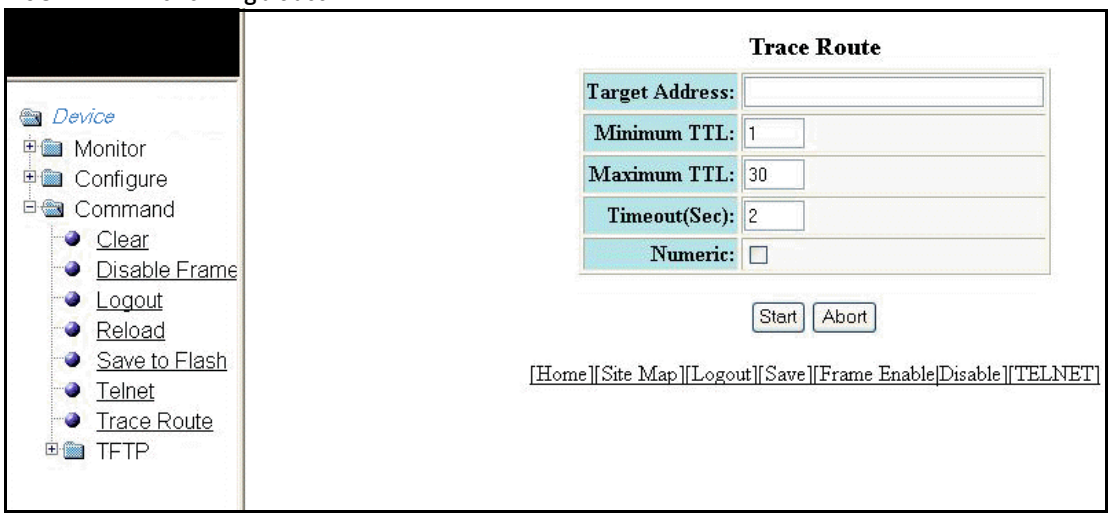
Performing a trace

Trace Route allows you to trace a path from the Brocade device to an IPv4 host. Trace route requests show all responses to a minimum Time To Live (TTL) of 1 second and a maximum TTL of 30 seconds. In addition, if there are multiple equal-cost routes to the destination, the Brocade device displays up to three responses. To run a trace, perform the following steps.

1. Click **Command** on the left pane and select **Trace Route**.

The **Trace Route** window is displayed as shown in Figure 222.

FIGURE 222 Performing a trace



2. Type the IP address of the host at the other end of the route in the **Target Address** field.
3. Type the minimum value of TTL in the **Minimum TTL** field. The default is one.
4. Type the maximum value of TTL in the **Maximum TTL** field. The default is 30.
5. Type the number of seconds the router waits for a reply from the pinged device in the **Timeout (Sec)** field.
6. Select the **Numeric** check box so that, for parameters that require a numeric value, the trace route does not check that the value you enter is within the allowed range. Instead, if you do exceed the range for a numeric value, the software rounds the value to the nearest valid value.
7. Click **Start** to begin the trace process or click **Abort** to exit without performing the trace.

Chapter

33

Using TFTP

In this chapter

- Configuring TFTP 317
- Configuring a TFTP image 318

Configuring TFTP

When the device reboots, or the auto-configuration feature has been disabled and then re-enabled, the device uses information from the Dynamic Host Configuration Protocol (DHCP) server to contact the Trivial File Transfer Protocol (TFTP) server to update the running configuration file. If the DHCP server provides a TFTP server name or IP address, the device uses this information to request files from the TFTP server. If the DHCP server does not provide a TFTP server name or IP address, the device requests the configuration files from the DHCP server.

The device requests the configuration files from the TFTP server in the following order:

- Boot file name provided by the DHCP server (if configured)
- Host name MAC address configuration file
- Brocade configuration file

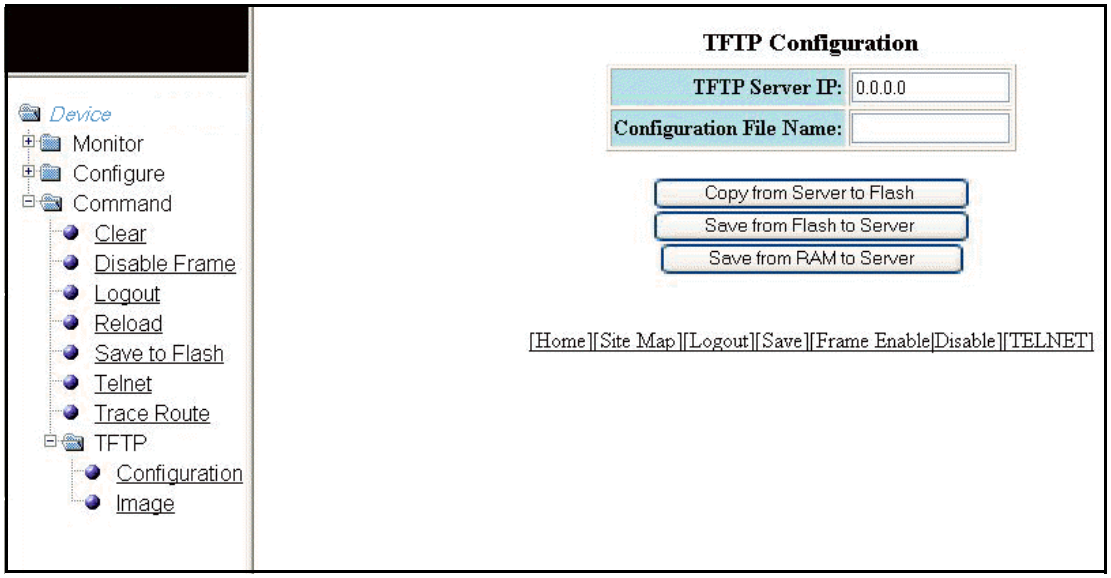
If the device is successful in contacting the TFTP server and the server has the configuration files, the files are merged. If there is a conflict, the server file takes precedence. If the device is unable to contact the TFTP server or if the files are not found on the server, the TFTP part of the configuration download process ends.

To access the TFTP configuration, perform the following steps.

1. Click **Command** on the left pane and select **TFTP**.
2. Click **Configuration**.

The **TFTP Configuration** window is displayed as shown in Figure 223.

FIGURE 223 Configuring TFTP



3. Type the IP address of the most recently contacted TFTP server (if the switch has contacted a TFTP server since the last time the software was reloaded or the switch was rebooted) in the **TFTP Server IP** field.
4. Type the name under which the startup-config file of the Layer 2 switch or Layer 3 switch was uploaded or downloaded during the most recent TFTP access in the **Configuration File Name** field.
5. You can perform one of the following tasks with the configuration file:
   - Click **Copy from Server to Flash** to copy the file from a TFTP server to the device flash memory.
   - Click **Save from Flash to Server** to save the file from the device flash memory to a TFTP server.
   - Click **Save from RAM to Server** to save the file from the device RAM memory to a TFTP server.

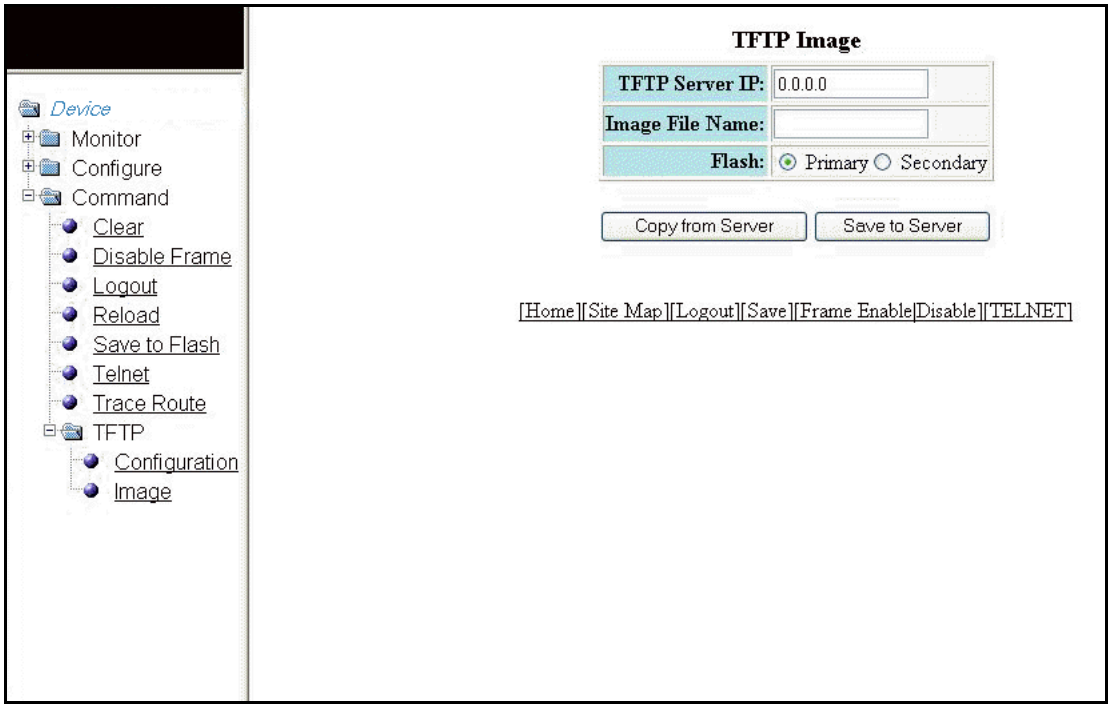
Configuring a TFTP image

To access a TFTP image, perform the following steps.

1. Click **Command** on the left pane and select **TFTP**.
2. Click **Image**.

The **TFTP Image** window is displayed as shown in Figure 224.

FIGURE 224 Configuring a TFTP image



3. Type the IP address of the most recently contacted TFTP server (if the switch has contacted a TFTP server since the last time the software was reloaded or the switch was rebooted) in the **TFTP Server IP** field.
4. Type the name of the Layer 2 switch or Layer 3 switch flash image (system software file) that was uploaded or downloaded during the most recent TFTP access in the **Image File Name** field.
5. Click one of the following for **Flash**:
   - **Primary** - The default local storage device for image files and configuration files.
   - **Secondary** - The second flash storage device you can use to store redundant images for additional booting reliability or to preserve one software image while testing another one.
6. You can perform one of the following tasks with the TFTP image:
   - Click **Copy from Server** to copy a boot image from a TFTP server to the primary or secondary storage location in the device flash memory.
   - Click **Save to Server** to save the boot image from the primary or secondary storage location of the device flash memory to a TFTP server.